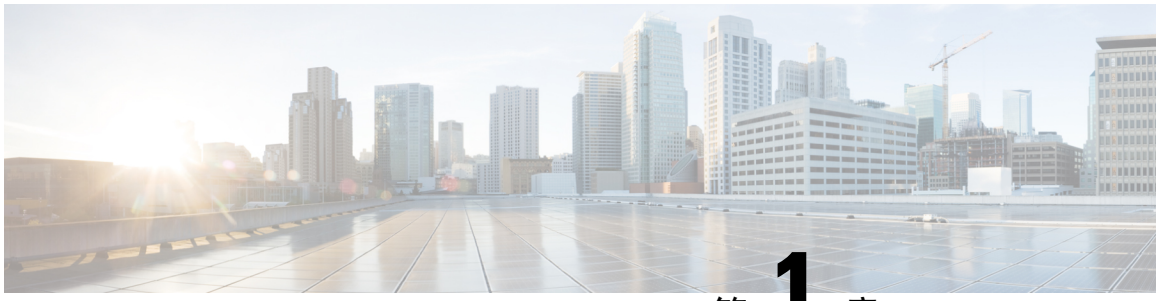
思科 **AnyConnect** 安全移动客户端管理员指南，**4.10** 版

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



第 1 章

部署 AnyConnect

开始部署前

如果您正在部署 Umbrella 漫游安全模块，系统将自动检测并删除现已安装的所有 Umbrella 漫游客户端，以防止冲突。如果现已安装的 Umbrella 漫游客户端与某项 Umbrella 服务订用相关联，会将该项服务订用自动迁移至 Umbrella 漫游安全模块，除非 OrgInfo.json 文件与配置用于网络部署或预部署的 AnyConnect 安装程序处于 Umbrella 模块目录中的同一位置。您可能希望在部署 Umbrella 漫游安全模块之前手动卸载 Umbrella 漫游客户端。

此外，如果使用 Umbrella 漫游安全模块，您还必须完成以下前提条件：

- **获得 Umbrella 漫游帐户**。Umbrella 控制面板 http://dashboard.umbrella.com 是登录页，您可在此获得操作 AnyConnect Umbrella 漫游安全模块的必要信息。您还可以使用此站点来管理对漫游客户端活动的报告。
- **从控制面板下载 OrgInfo 文件**。要为部署 AnyConnect Umbrella 漫游安全模块做好准备，请从 Umbrella 控制面板获取 OrgInfo.json 文件。单击“身份 (Identities)”菜单结构中的**漫游计算机 (Roaming Computer)**，然后单击页面左上角的 + 符号。向下滚动到 AnyConnect Umbrella 漫游安全模块并单击**模块配置文件 (Module Profile)**。

  OrgInfo.json 文件包含关于您的 Umbrella 服务订用的具体信息，可让漫游安全模块了解向哪里报告，以及需要实施哪些策略。

AnyConnect 部署概述

部署 AnyConnect 是指安装、配置和升级 AnyConnect 客户端及其相关文件。

Cisco AnyConnect Secure Mobility Client 可通过以下方法部署到远程用户：

- 预部署 - 新安装和升级可以由最终用户执行，也可以由企业软件管理系统 (SMS) 执行。
- 网络部署 - 将 AnyConnect 软件包载入头端，即 ASA 或 FTD 防火墙或者 ISE 服务器。当用户连接到防火墙或 ISE 时，则会将 AnyConnect 部署到客户端。
  - 对于新安装，用户可连接到前端以下载 AnyConnect 客户端。客户端可手动或自动安装（通过网络启动）。
  - 更新由已安装 AnyConnect 的系统上运行的 AnyConnect 完成，或者通过将用户定向至 ASA 无客户端门户完成。
- 云更新 - 在部署 Umbrella 漫游安全模块后，可以使用上述方法之一以及云更新来更新任何 AnyConnect 模块。通过云更新，可自动从 Umbrella 云基础设施获得软件升级，且更新跟踪将取决于该软件升级，而非管理员的任何操作。默认情况下，将禁用通过云更新进行自动更新。

注释 需要考虑以下有关云更新的情况：

- 只会更新当前安装的软件模块。
- 不支持定制、本地化和任何其他部署类型。
- 更新仅在登录到桌面时才会进行，如果建立了 VPN，则不会进行更新。
- 当禁用更新时，最新软件功能和更新将不可用。
- 禁用云更新对其他更新机制或设置（例如网络部署、延迟更新等）没有影响。
- 云更新将忽略装有较新、未发布的版本（例如临时版本和修补版本）AnyConnect 的设备。

部署 AnyConnect 时，您可以启用额外功能的可选模块以及用于配置 VPN 和可选功能的客户端配置文件。

有关 ASA、IOS、Microsoft Windows、Linux 和 macOS 的系统、管理和终端要求，请参阅 AnyConnect 版本说明。

注释 有些第三方应用和操作系统可能会限制 ISE 终端安全评估代理和其他进程进行必要的文件访问和权限提升。确保 AnyConnect 安装目录（在 Windows 中目录是 C:\Program Files (x86)\Cisco，在 macOS 中目录是 /opt/cisco）受信任并/或位于终端防病毒、反恶意软件、反间谍软件、防数据丢失、权限管理器或组策略对象的允许/排除/信任列表中。

此外，第三方安全应用程序 (AV/AS/AM/DLP) 可能会导致合规模块升级失败，这是因为交互会导致终端上缺少库。要避免这些问题，可在升级合规模块之前升级合规模块版本并将这些设为排除（在第三方安全应用程序中）：

```
-anyconnect-win-4.3.xxxx.xxxx-isecompliance-webdeploy-k0.pkg
-anyconnect-win-4.3.xxxx.xxxx-isecompliance-webdeploy-k9.exe
-anyconnect-win-4.3.xxxx.xxxx-isecompliance-webdeploy-k9.msi
-opswat.msi
```

决定如何安装 AnyConnect

AnyConnect 可以由 ISE 2.0（或更高版本）和 ASA 头端进行网络部署，或者进行预部署。安装 AnyConnect 最初需要管理权限。

网络部署

要使用网络部署（从含下载程序的 ASA/ISE/Umbrella 云）升级 AnyConnect 或安装额外模块，您不需要管理权限。

- 从 ASA 或 FTD 设备进行网络部署 - 用户连接到头端设备上的 AnyConnect 无客户端网络门户，然后选择下载 AnyConnect。ASA 下载 AnyConnect 下载程序。AnyConnect 下载程序下载客户端，安装客户端，并启动 VPN 连接。
- 从 ISE 进行网络部署 - 用户连接到网络访问设备 (NAD)，例如 ASA、无线控制器或交换机。NAD 授权用户，并将用户重定向至 ISE 门户。将在客户端上安装 AnyConnect 下载程序，以管理软件包提取和安装，但不会启动 VPN 连接。

预部署

要使用预部署（手动或使用 SCCM 等进行带外部署）升级 AnyConnect 或安装额外模块，您需要管理权限。

- 使用企业软件管理系统 (SMS)。
- 手动分发 AnyConnect 文件存档，以及指导用户如何安装的说明。对于 Windows，文件存档格式是 zip；对于 macOS，是 DMG；对于 Linux，是 gzip。

有关系统要求和许可依赖性，请参阅《AnyConnect 安全移动客户端功能、许可证和操作系统指南》。

注释 如果您使用 AnyConnect 终端安全评估 (HostScan) 在 macOS 或 Linux 平台上执行根权限活动，我们建议您预部署 AnyConnect 终端安全评估。

确定安装 AnyConnect 所需的资源

部署 AnyConnect 需要多种类型的文件：

- AnyConnect 核心客户端，包含在 AnyConnect 软件包中。
- 支持额外功能的模块，包含在 AnyConnect 软件包中。
- 配置 AnyConnect 和额外功能的客户端配置文件，您可以创建这些配置文件。
- 如果您要定制或本地化部署，还可以使用语言文件、图像、脚本和帮助文件。
- AnyConnect ISE 终端安全评估和合规性模块 (OPSWAT)。

为 AnyConnect 准备终端

结合使用 AnyConnect 和移动宽带卡

某些 3G 卡在使用 AnyConnect 前需要执行配置步骤。例如，VZAccess Manager 有三种设置：

- 调制解调器手动连接
- 调制解调器自动连接（漫游时除外）
- 局域网适配器自动连接

如果选择**局域网适配器自动连接 (LAN adapter auto connect)**，请将首选项设置为 NDIS 模式。NDIS 是“永远在线”的连接，即使在 VZAccess 管理器关闭时，您仍可保持连接状态。当 VZAccess 管理器为 AnyConnect 安装准备就绪时，它将自动连接局域网适配器显示为设备连接首选项。当检测到 AnyConnect 接口时，3G 管理器将丢弃接口并允许 AnyConnect 连接。

当您进入更高优先级的连接时（有线网络的优先级最高，WiFi 次之，最后是移动宽带），AnyConnect 将在断开旧连接之前建立新连接。

在 Windows 上将 ASA 添加到 Internet Explorer 的受信任站点列表

Active Directory 管理员可以使用组策略将 ASA 添加到 Internet Explorer 中的受信任站点列表。此过程不同于本地用户在 Internet Explorer 中添加受信任站点的方式。

步骤 1 在 Windows 域服务器上，以域管理员组成员的身份登录。

步骤 2 打开 Active Directory 用户和计算机 MMC 管理单元。

步骤 3 右键单击要在其中创建组策略对象的域或组织单元，然后单击**属性**。

步骤 4 选择**组策略** 选项卡，然后单击**新建**。

步骤 5 为新的组策略对象键入名称，并按 **Enter** 键。

步骤 6 为阻止这一新策略应用于某些用户或组，请单击**属性**。选择**安全性**选项卡。添加要禁止应用此策略的用户或组，然后在“允许”列中清除**读取**和**应用组策略**复选框。单击**确定**。

步骤 7 点击**编辑**并选择**用户配置** > **Windows 设置** > **Internet Explorer 维护** > **安全性**。

步骤 8 在右侧窗格中，右键单击**安全区域和内容分级**，然后单击**属性**。

步骤 9 选择**导入当前安全区域和隐私设置**。出现提示时，单击**继续**。

步骤 10 单击**修改设置**，选择**可信站点**，然后单击**站点**。

步骤 11 键入要添加到受信任站点列表的安全设备的URL，然后单击**添加**。格式可以包含主机名(https://vpn.mycompany.com)或 IP 地址 (https://192.168.1.100)。它可以是精确匹配 (https://vpn.mycompany.com) 或通配符 (https://*.mycompany.com)。

步骤 12 单击**关闭**，并连续单击**确定**，直至所有对话框都关闭。

步骤 13 留足时间让策略传播到整个域或林。

步骤 14 在“Internet 选项”窗口中单击 **确定**。

阻止 Internet Explorer 中的代理更改

某些情况下，AnyConnect 会隐藏（锁定）Internet Explorer 的“工具 > Internet 选项 > 连接”选项卡。显示此选项卡时，可让用户设置代理信息。隐藏此选项卡可防止用户有意或无意绕过隧道。断开连接后，该选项卡的锁定设置会撤消。选项卡锁定可被应用于该选项卡的任何管理员定义的策略覆盖。在以下情况下应用锁定：

- ASA 配置指定“连接”选项卡锁定
- ASA 配置指定专用端代理
- Windows 组策略之前锁定了“连接”选项卡（覆盖未锁定的 ASA 组策略设置）

对于 Windows 10 版本 1703（或更高版本），除了隐藏 Internet Explorer 中的“连接”选项卡外，AnyConnect 还会隐藏（锁定）“设置”应用中的“系统代理”选项卡，以防止用户故意或无意中绕过隧道。断开连接后，该锁定会撤消。

步骤 1 在 ASDM 中，转到**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **组策略 (Group Policies)**。

步骤 2 选择组策略，单击**编辑 (Edit)** 或**添加 (Add)** 可编辑或新增组策略。

步骤 3 在导航窗格中，转到**高级 (Advanced)** > **浏览器代理 (Browser Proxy)**。系统显示“代理服务器策略”(Proxy Server Policy) 窗格。

步骤 4 单击**代理锁定 (Proxy Lockdown)** 以显示更多代理设置。

步骤 5 取消选中**继承 (Inherit)** 并选择以下两个选项之一：

- **是**，将启用代理锁定，并在 AnyConnect 会话期间隐藏 Internet Explorer 的“连接”选项卡。
- **否**，将禁用代理锁定，并在 AnyConnect 会话期间显示 Internet Explorer 的“连接”选项卡。

步骤 6 单击**确定 (OK)** 保存代理服务器策略更改。

步骤 7 单击**应用 (Apply)** 保存组策略更改。

配置 AnyConnect 如何处理 Windows RDP 会话

可以将 AnyConnect 配置为允许来自 Windows RDP 会话的 VPN 连接。默认情况下，由 RDP 连接到计算机的用户无法启动使用 Cisco AnyConnect Secure Mobility Client 的 VPN 连接。下表显示来自 RDP 会话的 VPN 连接的登录和注销选项。这些首选项在 VPN 客户端配置文件中配置：

Windows 登录实施 (Windows Logon Enforcement) - 在 SBL 模式下可用

- 单一本地登录 (Single Local Logon)（默认设置）-（本地：1，远程：无限制）在整个 VPN 连接期间只允许一个本地用户登录。此外，当一个或多个远程用户登录到客户端 PC 时，本地用户可以建立 VPN 连接。此设置对通过 VPN 连接从企业网络登录的远程用户没有影响。

  注释 如果为全有或全无隧道配置了 VPN 连接，则修改 VPN 连接的客户端 PC 路由表会导致远程登录断开连接。如果 VPN 连接进行了分割隧道配置，远程登录可能会也可能不会断开连接，这取决于 VPN 连接的路由配置。

- 单一登录 (Single Logon) -（本地 + 远程：1）在整个 VPN 连接期间仅允许一个用户登录。如果通过本地或远程登录的用户不止一个，则在建立 VPN 连接时，将不允许该连接。如果 VPN 连接期间有第二个用户通过本地或远程登录，则 VPN 连接将终止。由于在 VPN 连接期间不允许进行其他登录，所以无法通过 VPN 连接进行远程登录。

  注释 不支持多个用户同时登录。

- 单一登录无远程 (Single Logon No Remote) -（本地：1，远程：0）在整个 VPN 连接期间只允许一个本地用户登录。不允许任何远程用户。如果在建立VPN连接后，有多个本地用户或任何远程用户登录，则将不允许此连接。如果VPN连接期间有第二个本地用户或任何远程用户登录，则此 VPN 连接将终止。

Windows VPN 建立 (Windows VPN Establishment) - 在 SBL 模式下不可用

- Local Users Only（默认值）- 阻止远程登录用户建立 VPN 连接。此功能与 AnyConnect 早期版本中的功能相同。
- Allow Remote Users - 允许远程用户建立 VPN 连接。但是，如果所配置的 VPN 连接路由导致远程用户断开连接，则 VPN 连接会终止，以允许远程用户重新获得对客户端 PC 的访问权限。如果远程用户想要断开其远程登录会话而不终止 VPN 连接，则必须在 VPN 建立后等待 90 秒钟。

有关其他 VPN 会话连接选项，请参阅 AnyConnect VPN 连接选项。

配置 AnyConnect 如何处理 Linux SSH 会话

可以将 AnyConnect 配置为允许来自 Linux SSH 会话的 VPN 连接。默认情况下，由 SSH 连接到计算机的用户无法启动使用 Cisco AnyConnect Secure Mobility Client 的 VPN 连接。下表显示来自 SSH 会话的 VPN 连接的登录和注销选项。这些选项在 VPN 客户端配置文件中配置。

Linux 登录实施 — 单点本地登录（默认值）：在整个 VPN 连接期间只允许一个本地用户登录。此外，当一个或多个远程用户登录到客户端 PC 时，本地用户可以建立 VPN 连接。此设置对通过 VPN 连接从企业网络登录的远程用户没有影响。

注释 如果为全有或全无隧道配置了 VPN 连接，则修改 VPN 连接的客户端 PC 路由表会导致远程登录断开连接。如果 VPN 连接进行了分割隧道配置，远程登录可能会也可能不会断开连接，这取决于 VPN 连接的路由配置。

单点登录 — 在整个 VPN 连接期间仅允许一个用户登录。如果通过本地或远程登录的用户不止一个，则在建立 VPN 连接时，将不允许该连接。如果 VPN 连接期间有第二个用户通过本地或远程登录，则 VPN 连接将终止。由于在 VPN 连接期间不允许进行其他登录，所以无法通过 VPN 连接进行远程登录。

Linux VPN 建立 —

- Local Users Only（默认值）- 阻止远程登录用户建立 VPN 连接。
- Allow Remote Users - 允许远程用户建立 VPN 连接。

有关其他 VPN 会话连接选项，请参阅 AnyConnect VPN 连接选项。

Windows 上仅使用 DES 的 SSL 加密

默认情况下，Windows 不支持 DES SSL 加密。如果在 ASA 上配置仅使用 DES，AnyConnect 连接将失败。由于很难将这些操作系统配置为使用 DES，因此建议不要将 ASA 配置为仅使用 DES 的 SSL 加密。

在 Linux 上使用 NVM

在 Linux 上使用 NVM 之前，必须设置内核驱动程序框架 (KDF)。您可以选择预构建 AnyConnect 内核模块或基于目标构建驱动程序。如果您选择基于目标构建，则无需任何操作；在部署或重新引导期间会自动处理构建。

构建 AnyConnect 内核模块的前提条件

准备目标设备：

- 确保已安装 GNU Make Utility。

- 安装内核报头软件包：
  - 对于 RHEL，请安装软件包 **kernel-devel-$(uname -r)**，例如 kernel-devel-2.6.32-642.13.1.el6.x86_64。
  - 对于 Ubuntu，请安装软件包 **linux-headers-$(uname -r)**，例如 linux-headers-4.2.0-27-generic。
  - 对于 Linux，安装所需的 libelf devel 软件包。
- 确保已安装 GCC 编译器。已安装 GCC 编译器的 *major.minor* 版本应与用来构建内核的 GCC 版本相匹配。您可在 /proc/version 文件中对其进行验证。

将 NVM 与预构建的 AnyConnect Linux 内核模块打包在一起

开始之前

完成构建 AnyConnect 内核模块的前提条件，第 7 页中的前提条件。

AnyConnect NVM 可以通过预构建的 AnyConnect Linux 内核模块进行打包，因此您不需要在每个目标设备上建立它，尤其是当目标设备具有相同的操作系统内核版本时。如果您决定不使用预构建选项，则可以在目标上使用，这在部署或重新引导期间自动发生，无需管理员输入。或者，如果您的部署在所有终端上没有内核先决条件，可以使用预构建选项。

注释　预构建的 AnyConnect Linux 内核模块不支持 Web 部署。

步骤 1　提取 AnyConnect 预部署软件包：anyconnect-linux64-<版本>-predeploy-k9.tar.gz。

步骤 2　导航到 nvm 目录。

步骤 3　调用脚本 **$sudo ./build_and_package_ac_ko.sh**。

在运行脚本后，将创建 anyconnect-linux64-<版本>**-ac_kdf_ko-k9.tar.gz**，其包括 AnyConnect Linux 内核模块版本。在启用安全启动的系统上，使用安全启动所允许的专用密钥对模块进行签名。此文件仅可用于预部署。

下一步做什么

升级目标设备的操作系统内核时，必须通过更新的 Linux 内核模块重新部署 AnyConnect NVM。

预部署 AnyConnect

可使用 SMS 预部署 AnyConnect，方法是手动为最终用户分发要安装的文件或向用户提供 AnyConnect 文件存档以供连接。

当创建文件存档以安装 AnyConnect 时，存档的目录结构必须与客户端上安装的文件的目录结构一致，如以下章节所述： 预部署 AnyConnect 配置文件的位置，第 10 页

开始之前

- 如果手动部署VPN配置文件，还必须将配置文件上传到头端。当客户端系统连接时，AnyConnect会验证客户端上的配置文件是否与头端上的配置文件匹配。如果已禁用配置文件更新，并且头端上的配置文件与客户端上的配置文件不同，则手动部署的配置文件将不起作用。
- 如果手动部署 AnyConnect ISE 终端安全评估配置文件，您还必须将该文件上传到 ISE。
- 如果您使用的是克隆虚拟机，请参考 克隆虚拟机配合使用 AnyConnect 指南（仅限 Windows），第 12 页。

步骤 1 下载 AnyConnect 预部署软件包。

用于预部署的 AnyConnect 文件在 cisco.com 上提供。

操作系统	**AnyConnect** 预部署软件包名称
Windows 的 ISE 安全评估代理	anyconnect-win-版本-predeploy-k9.zip
macOS	anyconnect-macos-*version*-predeploy-k9.dmg
Linux（64位）	anyconnect-linux64-版本-predeploy-k9.tar.gz

Umbrella 漫游安全模块不可用于 Linux 操作系统。

步骤 2 创建客户端配置文件：某些模块和功能需要客户端配置文件。

以下模块需要客户端配置文件：

- AnyConnect VPN
- 思科 AnyConnect 网络访问管理器
- AnyConnect ISE 终端安全评估
- AnyConnect AMP 启用程序
- 网络可视性模块
- Umbrella 漫游安全模块

以下模块不需要 AnyConnect 客户端配置文件：

- AnyConnect VPN 登录前开始
- AnyConnect 诊断和报告工具
- AnyConnect 终端安全评估
- AnyConnect 客户体验反馈

可在 ASDM 中创建客户端配置文件，并将这些文件复制到您的 PC。或者，您可以使用 Windows PC 上的独立配置文件编辑器。

步骤 3 或者定制和本地化 AnyConnect 客户端和安装程序，第 39 页。

步骤 4 准备分发的文件。这些文件的目录结构在预部署 AnyConnect 配置文件的位置中进行了描述。

步骤 5 创建 AnyConnect 安装所需的所有文件后，可将它们分发在一个存档文件中，或将这些文件复制到客户端。确保您计划连接到的头端（ASA 和 ISE）上也有相同的 AnyConnect 文件。

用于预部署和网络部署的 AnyConnect 模块可执行文件

下表列出了在将 Umbrella 漫游安全模块、网络访问管理器、AMP 启用程序、ISE 终端安全评估及 Network Visibility Module 客户端预部署或网络部署到 Windows 计算机时终端计算机上的文件名。

表 *1:* 网络部署或预部署的模块文件名

模块	网络部署安装程序（已下载）	预部署安装程序
网络访问管理器	anyconnect-win-版本-nam-webdeploy-k9.msi	anyconnect-win-版本-nam-predeploy-k9.msi
ISE 终端安全评估	anyconnect-win-版本-iseposture-webdeploy-k9.msi	anyconnect-win-版本-iseposture-predeploy-k9.msi
AMP Enabler	anyconnect-win-版本-amp-webdeploy-k9.msi	anyconnect-win-版本-amp-predeploy-k9.exe
网络可视性模块	anyconnect-win-*version*-nvm-webdeploy-k9.exe	anyconnect-win-*version*-nvm-predeploy-k9.msi
Umbrella 漫游安全模块	anyconnect-win-*version*-umbrella-webdeploy-k9.exe	anyconnect-win-*version*-umbrella-predeploy-k9.msi

AnyConnect 4.3（及更高版本）已移至 Visual Studio (VS) 2015 版本环境，并且需要可再分发的 VS 文件以实现其网络访问管理器模块的功能。这些文件作为安装文件包的组成部分安装。您可以使用 .msi 文件将网络访问管理器模块升级到 4.3（或更高版本），但必须先升级 AnyConnect 安全移动客户端并运行版本 4.3（或更高版本）。

注释 如果有 Windows 服务器操作程序，在尝试安装 AnyConnect 网络访问管理器时，可能会发生安装错误。默认情况下，服务器操作系统上未安装 WLAN 服务，因此，您必须安装并重新启动 PC。网络访问管理器要在任何 Windows 操作系统上正常运行，必须具备 WLANAutoconfig 服务。

预部署 AnyConnect 配置文件的位置

如果要将文件复制到客户端系统，下表显示您必须将文件放置到的位置。

表 *2: AnyConnect* 核心文件

文件	描述
anyfilename.xml	AnyConnect 配置文件。此文件指定了为特定用户类型配置的功能和属性值。
AnyConnectProfile.xsd	定义 XML 架构格式。AnyConnect 使用此文件验证配置文件。

表 *3:* 所有操作系统的配置文件位置

操作系统	模块	位置
Windows	使用 VPN 的核心客户端	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	网络访问管理器	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\newConfigFiles
	客户体验反馈	%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback
	OPSWAT	%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\opswat
	ISE 终端安全评估	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture
	AMP Enabler	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\AMP Enabler
	网络可视性模块	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM
	Umbrella 漫游安全模块	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella **注释** 要启用 Umbrella 漫游安全模块，必须从 Umbrella 控制面板中复制 OrgInfo.json 文件，并将其放置到此目标目录中，而不进行任何重命名。也可以将 OrgInfo.json 文件与 Umbrella 漫游安全模块安装程序放在同一位置，在安装前将该文件放置到 \Profiles\umbrella 中。

操作系统	模块	位置
macOS	所有其他模块	/opt/cisco/anyconnect/profile
	客户体验反馈	/opt/cisco/anyconnect/CustomerExperienceFeedback
	二进制文件	/opt/cisco/anyconnect/bin
	OPSWAT	/opt/cisco/anyconnect/lib/opswat
	库	/opt/cisco/anyconnect/lib
	用户界面资源	/Applications/Cisco/Cisco Secure Mobility Client.app/Contents/Resources/
	ISE 终端安全评估	/opt/cisco/anyconnect/iseposture/
	AMP Enabler	/opt/cisco/anyconnect/ampenabler/
	网络可视性模块	/opt/cisco/anyconnect/NVM/
	Umbrella 漫游安全模块	/opt/cisco/anyconnect/umbrella 注释 要启用 Umbrella 漫游安全模块，必须从 Umbrella 控制面板中复制 OrgInfo.json 文件，并将其放置到此目标目录中，而不进行任何重命名。也可以将 OrgInfo.json 文件与 Umbrella 漫游安全模块安装程序放在同一位置，在安装前将该文件放置到 \Profiles\umbrella 中。
Linux	NVM	/opt/cisco/anyconnect/NVM
	所有其他模块	/opt/cisco/anyconnect/profile

克隆虚拟机配合使用 AnyConnect 指南（仅限 Windows）

AnyConnect 终端由 AnyConnect 所有模块均使用的通用设备标识符 (UDID) 进行唯一标识。当对 Windows 虚拟机进行克隆时，源中所有克隆的 UDID 保持不变。要避免克隆虚拟机出现任何潜在问题，请在使用 AnyConnect 之前执行此操作：

1. 导航至 **C:\Program Files\Cisco\Cisco AnyConnect Secure MobilityClient**，并以管理员权限运行 dartcli.exe，如下所示：

   ```
   dartcli.exe -nu
   ```

   或

   ```
   dartcli.exe -newudid
   ```

2. 在执行此命令之前和之后打印 UDID，以确保 UDID 已通过此命令进行了更改：

   ```
   dartcli.exe -u
   ```

   或

```
dartcli.exe -udid
```

将 AnyConnect 模块预部署为独立应用

网络访问管理器、网络安全和 Umbrella 漫游安全模块可作为独立应用运行。安装 AnyConnect 核心客户端，但不使用 VPN 和 AnyConnect UI。

在 Windows 上使用 SMS 部署独立模块

步骤 1 通过配置软件管理系统 (SMS) 来设置 MSI 属性 PRE_DEPLOY_DISABLE_VPN=1，从而禁用 VPN 功能。例如：

```
msiexec /package anyconnect-win-版本-predeploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx*
<log_file_name>
```

MSI 将其中嵌入的 VPNDisable_ServiceProfile.xml 文件复制到为 VPN 功能的配置文件指定的目录。

步骤 2 安装模块。例如，以下 CLI 命令安装 Umbrella：

```
msiexec /package anyconnect-win-version-umbrella-predeploy-k9.msi /norestart /passive /lvx* c:\test.log
```

步骤 3 （可选）安装 DART。

misexec /package annyconnect-win-*version*-dart-predeploy-k9.msi /norestart /passive /lvx* c:\test.log

步骤 4 将经过模糊处理的客户端配置文件的副本保存到适当的 Windows 文件夹。

步骤 5 重新启动思科 AnyConnect 服务。

将 AnyConnect 模块部署为独立应用

独立 NVM，第 216 页有关其部署的优点和方法的详细信息，请参阅。

要求

VPNDisable_ServiceProfile.xml 文件还必须是在 VPN 客户端配置文件目录中的唯一 AnyConnect 配置文件。

独立模块的用户安装

您可以手动拆分各个安装程序并将它们分发给用户。

如果您决定向用户提供 zip 映像并要求他们安装，请务必向用户说明仅安装独立模块。

注释 如果计算机中此前未安装网络访问管理器，用户必须重启计算机才能完成网络访问管理器安装。此外，如果安装属于需要升级某些系统文件的升级安装，用户也必须重启计算机。

步骤 1 指导用户选中 AnyConnect 网络访问管理器或 Umbrella 漫游安全模块。

步骤 2 指导用户取消选中**思科AnyConnect VPN 模块 (Cisco AnyConnect VPN Module)**。

这将禁用核心客户端的 VPN 功能，安装实用程序将网络访问管理器或 Umbrella 漫游安全模块作为不含 VPN 功能的独立应用来安装。

步骤 3 （可选）选中**锁定组件服务 (Lock Down Component Services)** 复选框。锁定组件服务将阻止用户关闭或停止 Windows 服务。

步骤 4 指导用户运行可选模块的安装程序，这些模块可在没有 VPN 服务的情况下使用 AnyConnect GUI。如果用户单击“安装已选定”(Install Selected) 按钮，将发生以下情况：

a) 弹出一个对话框，要求确认独立网络访问管理器或 Umbrella 漫游安全模块的选择。
b) 如果用户单击“确定”(OK)，安装实用程序将使用 PRE_DEPLOY_DISABLE_VPN=1 设置调用 AnyConnect 核心安装程序。
c) 安装实用程序将删除所有现有 VPN 配置文件，然后安装 VPNDisable_ServiceProfile.xml。
d) 安装实用程序将调用网络访问管理器或 Umbrella 漫游安全安装程序。
e) 计算机将启用网络访问管理器或 Umbrella 漫游安全模块，但不含 VPN 服务。

预部署到 Windows

使用 zip 文件分发 AnyConnect

zip 软件包文件包含安装实用程序（用于启动单个组件安装程序的选择器菜单程序）以及核心和可选 AnyConnect 模块的 MSI。将 zip 软件包文件提供给用户后，用户运行安装程序 (setup.exe)。该程序显示安装实用程序菜单，用户从中选择要安装的 AnyConnect 模块。您可能不希望用户选择要加载哪些模块。因此，如果您决定使用 zip 进行分发，请编辑 zip 以删除不想使用的模块，然后编辑 HTA 文件。

分发 ISO 的一种方法是使用虚拟 CD 挂载软件，如 SlySoft 或 PowerIS。

预部署 zip 修改

- 使用您在捆绑文件时创建的配置文件更新 zip 文件，并删除不希望分发的任何模块安装程序。
- 编辑 HTA 文件可对安装菜单进行个性化设置，并删除到不希望分发的任何模块安装程序的链接。

AnyConnect zip 文件内容

文件	目的
GUI.ico	AnyConnect 图标图像。
Setup.exe	启动安装实用程序。

文件	目的
anyconnect-win-版本-dart-predeploy-k9.msi	DART 模块的 MSI 安装程序文件。
anyconnect-win-版本-gina-predeploy-k9.msi	SBL 模块的 MSI 安装程序文件。
anyconnect-win-版本-iseposture-predeploy-k9.msi	ISE 终端安全评估模块的 MSI 安装程序。
anyconnect-win-版本-amp-predeploy-k9.exe	AMP 启用程序的 MSI 安装程序文件。
anyconnect-win-版本-nvm-predeploy-k9.msi	网络可视性模块的 MSI 安装程序文件。
anyconnect-win-版本-umbrella-predeploy-k9.msi	Umbrella 漫游安全模块的 MSI 安装程序文件。
anyconnect-win-版本-nam-predeploy-k9.msi	网络访问管理器模块的 MSI 安装程序文件。
anyconnect-win-版本-posture-predeploy-k9.msi	终端安全评估模块的 MSI 安装程序文件。
anyconnect-win-版本-core-vpn-predeploy-k9.msi	AnyConnect 核心客户端的 MSI 安装程序文件。
autorun.inf	setup.exe 的信息文件。
eula.html	可接受使用策略。
setup.hta	安装实用程序 HTML 应用 (HTA)，您可以针对自己的站点进行定制。

使用 SMS 分发 AnyConnect

从 zip 映像提取要部署的模块的安装程序 (*.msi) 后，可以手动分发这些安装程序。

要求

- 在 Windows 上安装 AnyConnect 时，必须禁用 AlwaysInstallElevated 或 Windows 用户帐户控制 (UAC) 组策略设置。否则，AnyConnect 安装程序可能无法访问安装所需的某些目录。
- Microsoft Internet Explorer (MSIE) 用户应将头端添加到受信任站点列表或安装 Java。添加到受信任站点列表会启用 ActiveX 控件进行安装，此时用户交互最少。

配置文件部署过程

- 如果使用 MSI 安装程序，MSI 将选择已放置在 Profiles 文件夹中的任何配置文件并在安装过程中将其放置在相应的文件夹中。在 CCO 上可用的预部署 MSI 文件中会提供适当的文件夹路径。
- 如果在安装后手动预部署配置文件，请手动复制配置文件或使用 SMS（如 Altiris）将配置文件部署到相应的文件夹。
- 确保放到头端上的客户端配置文件与预部署到客户端的客户端配置文件相同。还必须将此配置文件绑定到 ASA 上使用的组策略。如果该客户端配置文件与头端上的客户端配置文件不匹配，或者如果没有将其绑定到组策略，则您可能获得不一致的行为，包括访问被拒绝。

Windows 预部署 MSI 示例

已安装的模块	命令和日志文件
无 VPN 功能的 AnyConnect 核心客户端。	msiexec /package anyconnect-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* anyconnect-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
有 VPN 功能的 AnyConnect 核心客户端。	msiexec /package anyconnect-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
客户体验反馈	msiexec /package anyconnect-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* anyconnect-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
诊断和报告工具 (DART)	msiexec /package anyconnect-win-*version*-dart-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-dart-predeploy-k9-install-datetimestamp.log
SBL	msiexec /package anyconnect-win-*version*-gina-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-gina-predeploy-k9-install-datetimestamp.log
网络访问管理器	msiexec /package anyconnect-win-*version*-nam-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-nam-predeploy-k9-install-datetimestamp.log
VPN 终端安全评估 (HostScan)	msiexec /package anyconnect-win-*version*-posture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-posture-predeploy-k9-install-datetimestamp.log
ISE 终端安全评估	msiexec /package anyconnect-win-*version*-iseposture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-iseposture-predeploy-k9-install-datetimestamp.log
AMP Enabler	msiexec /package anyconnect-win-*version*-amp-predeploy-k9.msi / norestart/passive /lvx*
网络可视性模块	msiexec /package anyconnect-win-*version*-nvm-predeploy-k9.msi / norestart/passive /lvx* anyconnect-win-*version*-nvm-predeploy-k9-install-datetimestamp.log
Umbrella 漫游安全	msiexec /package anyconnect-win-*version*-umbrella-predeploy-k9.msi / norestart/passive /lvx* anyconnect-*version*-umbrella-predeploy-k9-install-datetimestamp.log

AnyConnect 示例 Windows 转换

思科提供示例 Windows 转换以及介绍如何使用转换的文档，以下划线字符 (_) 开头的转换是一般 Windows转换，它允许您仅将某些转换应用于某些模块安装程序。以字母字符开头的转换是VPN转换。每个转换都有使用说明文档，转换下载说明文档是 sampleTransforms-*x.x.x*.zip。

Windows 预部署安全选项

思科建议授予最终用户对托管Cisco AnyConnect Secure Mobility Client的设备的有限权限。如果最终用户确保其他权利，则安装程序可提供锁定功能，防止用户和本地管理员关闭或停止终端上建立为锁定的 Windows 服务。您还可以阻止用户卸载 AnyConnect。

Windows 锁定属性

每个 MSI 安装程序都支持通用属性 (LOCKDOWN)，当该属性设置为非零值时，可防止与安装程序相关的 Windows 服务被终端设备上的用户或本地管理员控制。我们建议您使用安装时提供的示例转换 (anyconnect-vpn-transforms-X.X.xxxxx.zip) 来设置该属性，并将转换应用至您想锁定的每个 MSI 安装程序。锁定选项同样是 ISO 安装实用程序中的一个复选框。

从添加/删除程序列表中隐藏 AnyConnect

您可以隐藏安装的 AnyConnect 模块，这样用户从 Windows Add/Remove Program 列表中便看不到该模块。即使您使用 ARPSYSTEMCOMPONENT=1 启动任何安装程序，该模块都不会显示在 Windows Add/Remove Program 列表中。

我们建议您使用我们提供的示例转换 (anyconnect-vpn-transforms-X.X.xxxxx.zip) 来设置此属性。将该转换应用于您希望隐藏的每个模块的每个 MSI 安装程序。

Windows 上的 AnyConnect 模块安装和删除顺序

模块安装程序在开始安装之前会确认其版本与核心客户端相同。如果版本不匹配，该模块不会安装，并且安装程序通知用户存在版本不匹配。如果您使用安装实用程序，则会构建软件包中的模块并将其封装在一起，且版本始终匹配。

步骤 1 按以下顺序安装 AnyConnect 模块：

a) 安装 AnyConnect 核心客户端模块，此过程会安装 GUI 和 VPN 功能（SSL 和 IPsec）。

在 Windows 和 macOS 中，已创建受限制的用户帐户 (ciscoacvpnuser)，以便仅在检测到启用了管理隧道功能时才实施最小特权原则。在 AnyConnect 卸载期间或安装升级过程中，此帐户会被删除。

b) 安装 AnyConnect 诊断和报告工具 (DART) 模块，以提供有关 AnyConnect 核心客户端安装的有用诊断信息。

c) 按任意顺序安装 Umbrella 漫游安全模块、Network Visibility Module、AMP 启用程序、SBL、网络访问管理器、终端安全评估模块或 ISE 合规性模块。

步骤 2 按以下顺序卸载 AnyConnect 模块：

a) 按任意顺序卸载 Umbrella 漫游安全模块、Network Visibility Module、AMP 启用程序、网络访问管理器、终端安全评估、ISE 合规性模块或 SBL。

b) 卸载 AnyConnect 核心客户端。

c) 最后卸载 DART。

如果卸载过程失败，DART 信息会很有用。

注释 根据设计，卸载 AnyConnect 后，某些 XML 文件仍然保留。

预部署到 macOS

在 macOS 上安装和卸载 AnyConnect

用于 macOS 的 AnyConnect 以 DMG 文件形式分发，其中包括所有 AnyConnect 模块。当用户打开 DMG 文件，然后运行 AnyConnect.pkg 文件时，系统会启动安装对话框，引导用户完成安装。在“安装类型”(Installation Type) 屏幕上，用户可以选择要安装的软件包（模块）。

AnyConnect 4.9.04xxx 是 macOS 11 上的最低要求版本。有关与 macOS 11 相关的 AnyConnect 更改的详细信息，请参阅附录：与 macOS 11 (Big Sur) 相关的 AnyConnect 更改 ，第 303 页。

要从您的分发中删除任何 AnyConnect 模块，可使用 Apple pkgutil 工具，并在通过 ACTransforms.xml 修改安装程序后签署软件包。您可以定制语言和外观，并且还可以修改和更改一些其他安装操作，如“定制”章节中的使用 ACTransform.xml 在 macOS 上自定义安装程序行为 ，第 46 页所述。

在 Mac OS 上安装 AnyConnect 模块作为独立应用

可以只安装 Network Visibility Module 或 Umbrella 漫游安全模块，而不含 VPN。不使用 VPN 和 AnyConnect UI。

以下过程通过安装独立配置文件编辑器、创建配置文件和将该配置文件添加到 DMG 软件包中，来说明如何定制这些模块。它还将 AnyConnect 用户界面设置为在启动时自动启动，这使 AnyConnect 可以为相应模块提供必要的用户和组信息。

步骤 1 从 Cisco.com 下载 Cisco AnyConnect Secure Mobility Client DMG 软件包。

步骤 2 打开文件访问安装程序。请注意，下载的映像是只读文件。

步骤 3 通过运行磁盘实用程序或使用终端应用以使安装程序映像可写入，如下所示：

```
hdiutil convert <source dmg> -format UDRW -o <output dmg>
```

步骤 4 在运行 Windows 操作系统的计算机上安装独立配置文件编辑器。作为定制安装或完全安装的组成部分，必须选择所需的 AnyConnect 模块。默认情况下不会安装这些模块。

步骤 5 启动配置文件编辑器并创建配置文件。

步骤 6 将配置文件适当保存为 `OrgInfo.json`（从您控制面板上获得的名称），放在安全位置。

a) 将指定的 .wso 文件从 Windows 设备复制到 macOS 相应文件夹路径下的安装程序数据包中（例如对于网络安全，路径为 `AnyConnect x.x.x/Profiles/NVM`）。或者对于 NVM 实例，使用如下所示的终端应用：

```
cp <path to the wso> \Volumes\"AnyConnect <VERSION>"\Profiles\nvm\
```

b) 在 macOS 安装程序中，转到 `AnyConnect x.x.x/Profiles` 目录并在 TextEdit 中打开 `ACTransforms.xml` 文件进行编辑。设定 `<DisableVPN>` 元素为 **true** 以确保不安装 VPN 的功能：

```
<ACTransforms>
```

```
<DisableVPN>true</DisableVPN>

</ACTransforms>
```

c) AnyConnect DMG 数据包现在已准备就绪，可分配给您的用户。

步骤 7 将配置文件相应地另存为 `NVM_ServiceProfile.xml` 或 `OrgInfo.json`（从您控制面板上获得的名称），放在安全位置。

对于这些模块，配置文件编辑器将为该配置文件创建另一个模糊处理的版本（例如 NVM，将创建 `NVM_ServiceProfile.wso`），并将其保存到与您保存该配置文件相同的位置（例如对于 NVM，将另存为 `NVM_ServiceProfile.xml`）。按照以下步骤操作，以完成模糊处理：

a) 将指定的 .wso 文件从 Windows 设备复制到 macOS 相应文件夹路径下的安装程序数据包中（例如对于 NVM，路径为 `AnyConnect x.x.x/Profiles/nvm`）。或者对于 NVM 实例，使用如下所示的终端应用：

```
cp <path to the wso> \Volumes\"AnyConnect <VERSION>"\Profiles\nvm\
```

b) 在 macOS 安装程序中，转到 `AnyConnect x.x.x/Profiles` 目录并在 TextEdit 中打开 `ACTransforms.xml` 文件进行编辑。设定 `<DisableVPN>` 元素为 **true** 以确保不安装 VPN 的功能：

```
<ACTransforms>

<DisableVPN>true</DisableVPN>

</ACTransforms>
```

c) AnyConnect DMG 数据包现在已准备就绪，可分配给您的用户。

在 macOS 上限制应用

Gatekeeper 可以限制允许哪些应用在系统上运行。您可选择允许从以下位置下载的应用：

- Mac App Store
- Mac App Store 和已确定的开发商
- 任何地点

默认设置为“Mac 应用商店和已确定的开发商”(Mac App Store and identified developers)（已签名的应用）。

AnyConnect 当前版本是使用 Apple 证书的已签名应用。如果（仅）面向 Mac App Store 配置 Gatekeeper，则您必须选择“任何地点”(Anywhere) 设置或按住 Ctrl 键单击，以绕过选定的设置，进而通过预部署的安装方式安装和运行 AnyConnect。有关详细信息，请参阅：http://www.apple.com/macosx/mountain-lion/security.html。

预部署到 Linux

安装用于 Linux 的模块

您可以打开用于 Linux 的单个安装程序并手动分配它们。预部署安装包中的各个安装程序均可以单独运行。使用压缩文件实用程序查看和提取 tar.gz 文件中的文件。

步骤 1 安装 AnyConnect 核心客户端模块，此过程会安装 GUI 和 VPN 功能（SSL 和 IPsec）。

步骤 2 安装 DART 模块，该模块提供关于 AnyConnect 核心客户端安装的有用诊断信息。

步骤 3 安装终端安全评估模块或 ISE 合规性模块。

步骤 4 安装 NVM。

卸载用于 Linux 的模块

用户卸载 AnyConnect 的顺序非常重要。

如果卸载过程失败，DART 信息将非常有价值。

步骤 1 卸载 NVM。

步骤 2 卸载终端安全评估模块或 ISE 合规性模块。

步骤 3 卸载 AnyConnect 核心客户端。

步骤 4 卸载 DART。

在 Linux 设备上手动安装/卸载 NVM

步骤 1 提取 AnyConnect 预部署软件包。

步骤 2 导航到 nvm 目录。

步骤 3 调用脚本 **$sudo ./nvm_install.sh**。

您可以使用 /opt/cisco/anyconnect/bin/nvm_uninstall.sh 卸载 NVM。

用于服务器证书验证的证书存储库

默认情况下，AnyConnect 使用 PEM 文件证书存储库，包括系统 CA 证书位置 (/etc/ssl/certs)，以便验证服务器证书。Firefox NSS 证书库也可用于 AnyConnect 验证服务器证书。

激活 Firefox NSS 证书存储库

如果您从未启动过在 Linux 设备上安装的 Firefox 浏览器，则必须首先创建 Firefox 用户配置文件，其中包括证书存储库。AnyConnect 会尝试将其用于服务器认证验证。

如果不使用 Firefox NSS 证书存储库

您必须将本地策略配置为排除 Firefox NSS 证书存储库，并且必须保持启用 PEM 文件证书存储库。

多模块要求

如果部署核心客户端以及一个或多个可选模块，则必须对每个安装程序应用锁定属性。Windows 预部署 MSI 示例，第 16 页介绍了锁定。

此操作可用于 VPN 安装程序、网络访问管理器、Network Visibility Module 和 Umbrella 漫游安全模块。

注释 如果选择激活对 VPN 安装程序的锁定，将因此也会锁定 AMP 启用程序。

在 Linux 设备上手动安装 DART

1. 将 anyconnect-dart-linux-(ver)-k9.tar.gz 存储在本地。
2. 从终端使用 **tar -zxvf** <含文件名的 *tar.gz* 文件路径命令提取 tar.gz 文件。
3. 从终端导航到提取的文件夹，并使用 **sudo ./dart_install.sh** 命令运行 dart_install.sh。
4. 接受许可协议，并等待安装完成。

注释 您仅可使用 **/opt/cisco/anyconnect/dart/dart_uninstall.sh** 卸载 DART。

网络部署 AnyConnect

网络部署是指客户端系统上的 AnyConnect 下载程序从头端获取 AnyConnect 软件，或使用头端上的门户安装或更新 AnyConnect。传统网络启动过于依赖浏览器支持（以及 Java 和 ActiveX 要求），作为一种替代方案，我们改进了自动网络部署的流程，该流程在初始下载以及从无客户端页面启动时会显示。自动调配 (Weblaunch) 仅适用于使用 Internet Explorer 浏览器的 Windows 操作系统。

通过 ASA 进行网络部署

ASA 上的无客户端门户执行 AnyConnect 网络部署。流程如下：

用户打开浏览器并连接到 ASA 的无客户端门户。在门户上，用户单击**启动 AnyConnect 客户端 (Start AnyConnect Client)** 按钮。然后，他们可以手动下载 AnyConnect 软件包。如果他们运行的浏览器支

持 NPAPI（Netscape 插件应用编程接口）插件，则还可以使用该选项卡通过 weblaunch（ActiveX 或 Java）来启动自动网络调配。

ASA 网络部署限制

- 不支持将同一 O/S 的多个 AnyConnect 软件包载入 ASA。
- 网络部署时，VPN 终端安全评估 (HostScan) 模块中不含 OPSWAT 定义。您必须手动部署 HostScan 模块或将其载入 ASA 上，以向客户端提供 OPSWAT 定义。
- 如果 ASA 只有默认内部闪存大小，您在 ASA 上存储和加载多个 AnyConnect 客户端软件包时可能会遇到问题。即使您的闪存有足够空间承载软件包，ASA 也可能会在解压缩和加载客户端映像时耗尽缓存内存。有关部署 AnyConnect 以及升级 ASA 内存时 ASA 内存要求的详细信息，请参阅最新的 VPN 设备版本说明。
- 用户可使用 IP 地址或 DNS 连接到 ASA，但不支持链路本地安全网关地址。
- 您必须将支持网络启动的安全设备的 URL 添加到 Internet Explorer 的受信任站点列表中。可使用组策略完成此操作，如在 Windows 上将 ASA 添加到 Internet Explorer 的受信任站点列表所述。
- 对于 Windows 7 SP1 用户，我们建议您在安装和首次使用之前安装 Microsoft .NET framework 4.0。在启动时，Umbrella 服务将检查是否已安装了 .NET framework 4.0（或更高版本）。如果未检测到，则不会激活 Umbrella 漫游安全模块，并将显示一条消息。下载然后安装 .NET Framework，必须重新启动才能激活 Umbrella 漫游安全模块。

通过 ISE 进行网络部署

ISE 上的策略确定 AnyConnect 客户端的部署时间。用户打开浏览器并连接到 ISE 控制的资源，然后重定向到 AnyConnect 客户端门户。该 ISE 门户将帮助用户下载和安装 AnyConnect。在 Internet Explorer 中，ActiveX 控件将指导用户进行安装。在其他浏览器中，门户将下载网络设置助理，该工具会帮助用户安装 AnyConnect。

ISE 部署限制

- 如果 ISE 和 ASA 均执行 AnyConnect 网络部署，则两个前端上的配置必须匹配。
- 如果在 ISE Client Provisioning Policy 中配置了 AnyConnect ISE 终端安全评估代理，则 ISE 服务器只能由该代理发现。ISE 管理员可在 Agent Configuration > Policy > Client Provisioning 下配置 NAC 代理或 AnyConnect ISE 终端安全评估模块。

在 ASA 上配置网络部署

下载 AnyConnect 软件包

从思科 AnyConnect 软件下载网页下载最新的 Cisco AnyConnect Secure Mobility Client软件包。

操作系统	AnyConnect 网络部署软件包名称
Windows 的 ISE 安全评估代理	anyconnect-win-版本-webdeploy-k9.pkg

操作系统	AnyConnect 网络部署软件包名称
macOS	anyconnect-macos-版本-webdeploy-k9.pkg
Linux（64位）	anyconnect-linux64-版本-webdeploy-k9.pkg

注释 您不应具有 ASA 上同一操作系统的不同版本。

在 ASA 上加载 AnyConnect 软件包

步骤 1 导航到 **Configuration**（配置） > **Remote Access**（远程访问） > **VPN** > **Network (Client) Access**（网络[客户端]访问） > **AnyConnect Client Software**（**AnyConnect 客户端软件**）。AnyConnect 客户端映像面板会显示当前在 ASA 上加载的 AnyConnect 映像。映像出现的顺序是 ASA 将其下载到远程计算机的顺序。

步骤 2 要添加 AnyConnect 映像，单击**添加 (Add)**。

- 单击**浏览闪存 (Browse Flash)** 可选择已上传到 ASA 的 AnyConnect 映像。
- 单击**上传 (Upload)** 浏览至您存储于本地计算机上的 AnyConnect 图像。

步骤 3 单击**确定 (OK)** 或**上传 (Upload)**。

步骤 4 单击**应用 (Apply)**。

启用其他 AnyConnect 模块

要启用其他功能，请在组策略或本地用户配置中指定新模块名称。注意启用附加模块将影响下载时间。启用功能时，AnyConnect 必须将这些模块下载到 VPN 终端。

注释 如果您选择“登录前开始”(Start Before Logon)，还必须在 AnyConnect 客户端配置文件中启用此功能。

步骤 1 在 ASDM 中，转到**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **组策略 (Group Policies)**。

步骤 2 选择组策略，单击**编辑 (Edit)** 或**添加 (Add)** 可编辑或新增组策略。

步骤 3 在导航窗格中，选择**VPN 策略 (VPN Policy)** > **AnyConnect 客户端 (AnyConnect Client)**。在**要下载的客户端模块 (Client Modules to Download)** 中，单击**添加 (Add)**，然后选择要添加到此组策略的每个模块。可用的模块是您添加或上传到 ASA 的模块。

步骤 4 单击**应用 (Apply)** 并保存对组策略的更改。

在 ASDM 中创建客户端配置文件

必须将 AnyConnect 网络部署软件包添加到 ASA，然后才能在 ASA 上创建客户端配置文件。

步骤 1 导航到**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **AnyConnect 客户端配置文件 (AnyConnect Client Profile)**。

步骤 2 选择要与组关联的客户端配置文件，然后单击**更改组策略 (Change Group Policy)**。

步骤 3 在“更改配置文件策略”(Change Policy for Profile) 策略名称窗口中，从“可用组策略”(Available Group Policies) 字段中选择组策略，然后单击右箭头，将其移到 Policies 字段。

步骤 4 单击**确定 (OK)**。

步骤 5 在“AnyConnect 客户端配置文件”(AnyConnect Client Profile) 页面上，单击**应用 (Apply)**。

步骤 6 单击**保存 (Save)**。

步骤 7 完成配置时，单击**确定 (OK)**。

在 ISE 上配置网络部署

ISE 可配置和部署 AnyConnect 核心、ISE 终端安全评估模块和 OPSWAT（合规性模块）以支持 ISE 的终端安全评估。ISE 还可以部署在连接到 ASA 时可使用的所有 AnyConnect 模块和资源。当用户浏览到 ISE 控制的资源时：

- 如果 ISE 在 ASA 之后，则用户连接 ASA，下载 AnyConnect，然后建立 VPN 连接。如果 AnyConnect ISE 终端安全评估并非由 ASA 安装，则用户将重定向到 AnyConnect 客户端门户来安装 ISE 终端安全评估。
- 如果 ISE 不在 ASA 之后，则用户连接到 AnyConnect 客户端门户，该门户会引导用户在 ISE 上安装 AnyConnect 配置中定义的 AnyConnect 资源。如果 ISE 终端安全评估状态未知，常见配置是将浏览器重定向到 AnyConnect 客户端调配门户。
- 当用户在 ISE 中被定向到 AnyConnect 客户端调配门户时：
  - 如果浏览器是 Internet Explorer，则 ISE 将下载 AnyConnect 下载程序，然后该下载程序会加载 AnyConnect。
  - 对于所有其他浏览器，ISE 将打开客户端调配重定向门户，该门户会显示下载网络设置助理 (NSA) 工具的链接。用户运行 NSA，该工具可查找 ISE 服务器并下载 AnyConnect 下载程序。

    NSA 在 Windows 上运行完毕后会自行删除。在 macOS 上运行完毕后，必须手动将其删除。

ISE 文档介绍了如何执行以下操作：

- 在 ISE 中创建 AnyConnect 配置文件
- 将 AnyConnect 资源从本地设备添加到 ISE
- 从远程站点添加 AnyConnect 调配资源

- 部署 AnyConnect 客户端和资源

注释 由于 AnyConnect ISE 终端安全评估模块在发现中不支持基于 Web 代理的重定向，思科建议您使用基于非重定向的发现。您可以在《思科身份服务引擎管理员指南》的“无需对不同网络进行 URL 重定向的客户端调配”部分中找到更多信息。

ISE 可配置和部署以下 AnyConnect 资源：

- AnyConnect 核心和模块，包括 ISE 终端安全评估模块
- 配置文件：Network Visibility Module、AMP 启用程序、VPN、网络访问管理器、客户反馈和 AnyConnect ISE 终端安全评估
- 定制文件
  - 用户界面资源
  - 二进制文件、连接脚本文件和帮助文件
- 本地化文件
  - 用于消息本地化的 AnyConnect gettext 转换
  - Windows Installer 转换

准备 AnyConnect 文件进行 ISE 上传

- 下载适用于操作系统的 AnyConnect 软件包，以及您希望在本地 PC 上部署的其他 AnyConnect 资源。

注释 对于 ASA，安装将使用 VPN 下载程序进行。在下载后，将通过 ASA 推送 ISE 终端安全评估配置文件，并在 ISE 终端安全评估模块联系 ISE 之前提供随后调配该配置文件所需的发现主机。而对于 ISE，ISE 终端安全评估模块只会在发现 ISE 后获取该配置文件，这有可能导致错误。因此，在连接到 VPN 时，建议使用 ASA 推送 ISE 终端安全评估模块。

- 为您计划部署的模块创建配置文件。至少创建一个 AnyConnect ISE 终端安全评估配置文件 (ISEPostureCFG.xml)。

注释 如果使用了基于非重定向的发现，则预部署 ISE 终端安全评估模块时必须使用包含 Call Home List 的 ISE 终端安全评估配置文件。

- 将定制和本地化资源合并成一个 ZIP 存档，该存档在 ISE 中称为捆绑包。捆绑包可包含：
  - AnyConnect UI 资源
  - VPN 连接脚本
  - 帮助文件
  - 安装程序转换

  AnyConnect 本地化捆绑包可包含：
  - 二进制格式的 AnyConnect Gettext 转换
  - 安装程序转换

按照准备 AnyConnect 定制和本地化进行 ISE 部署中所述的步骤创建 ISE 捆绑包。

配置 ISE 以部署 AnyConnect

必须先将 AnyConnect 软件包上传到 ISE，然后再上传和创建其他 AnyConnect 资源。

注释 在 ISE 中配置 AnyConnect 配置对象时，取消选中“AnyConnect 模块选择”(AnyConnect Module Selection) 下的 VPN 模块不会禁用已部署/已调配客户端上的 VPN。

1. 在 ISE 中，选择**策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (results)** > 。展开**客户端调配 (Client Provisioning)** 显示**资源 (Resources)**，然后选择**资源 (Resources)**。
2. 选择**添加 (Add)** > **本地磁盘代理资源 (Agent resources from local disk)**，然后上传 AnyConnect 软件包文件。为您计划部署的任何其他 AnyConnect 资源重复添加本地磁盘代理资源。
3. 选择**添加 (Add)** > **AnyConnect 配置 (AnyConnect Configuration)** > 。此 AnyConnect 配置用于对模块、配置文件、定制/语言包和 OPSWAT 软件包进行配置，如下表所述。

   可在 ISE、ASA 或 Windows AnyConnect 配置文件编辑器中创建和编辑 AnyConnect ISE 终端安全评估配置文件。下表显示 ISE 中每个 AnyConnect 资源的名称以及资源类型的名称。

表 *4: ISE* 中的 *AnyConnect* 资源

提示符	ISE 资源类型和说明
AnyConnect 软件包	AnyConnectDesktopWindows AnyConnectDesktopOSX AnyConnectWebAgentWindows AnyConnectWebAgentOSX
合规性模块	AnyConnectComplianceModuleWindows AnyConnectComplianceModuleOSX

提示符	ISE 资源类型和说明
AnyConnect 配置文件	AnyConnectProfile ISE 为上传的 AnyConnect 软件包所提供的每个配置文件显示一个复选框。
定制捆绑包	AnyConnectCustomizationBundle
本地化捆绑包	AnyConnectLocalizationBundle

4. 创建基于角色或基于操作系统的客户端调配策略。对于客户端调配终端安全评估代理，可选择 AnyConnect 和 ISE 传统 NAC/MAC 代理。每个客户端调配策略只能调配一个代理，要么是 AnyConnect 代理，要么是传统 NAC/MAC 代理。配置 AnyConnect 代理时，请选择一个在步骤 2 创建的 AnyConnect 配置。

在 FTD 上置网络部署

Firepower 威胁防御 (FTD) 设备是下一代防火墙 (NGFW)，提供类似于 ASA 的安全网关功能。FTD 设备仅支持使用 AnyConnect 安全移动客户端的远程接入 VPN (RA VPN)，不支持任何其他客户端或无客户端 VPN 接入。隧道建立和连接通过 IPsec IKEv2 或 SSL 完成。连接到 FTD 设备时不支持 IKEv1。

在 FTD 头端上配置 Windows、macOS 和 Linux AnyConnect 客户端，并在连接后进行部署，使远程用户能够访问 SSL 或 IKEv2 IPsec VPN 客户端，而无需安装和配置客户端软件。如果以前安装了客户端，当用户验证时，FTD 头端会检查客户端的版本，并根据需要升级客户端。

如果没有以前安装的客户端，远程用户需输入配置的接口 IP 地址，以下载和安装 AnyConnect 客户端。FTD 头端将下载和安装与远程计算机的操作系统匹配的客户端，并建立安全连接。

从平台应用程序商店可安装适用于 Apple iOS 和 Android 设备的 AnyConnect 应用程序。它们需要满足最低配置要求，以便与 FTD 头端建立连接。对于其他头端设备和环境，也可以使用本章介绍的另一种部署方法来分发 AnyConnect 软件。

目前，在 FTD 上只能配置核心 AnyConnect VPN 模块和 AnyConnect VPN 配置文件并将它们分发到终端。Firepower 管理中心 (FMC) 中的远程接入 VPN 策略向导可快速而轻松地设置这些基本 VPN 功能。

AnyConnect 和 FTD 的准则和局限性

- 唯一支持的 VPN 客户端是 Cisco AnyConnect Secure Mobility Client 。不支持任何其他客户端或本机 VPN。不支持使用无客户端 VPN 作为自己的实体；无客户端 VPN 仅用于部署 AnyConnect 客户端。
- 在 FTD 上使用 AnyConnect 需要版本 4.0 或更高版本的 AnyConnect，以及版本 6.2.1 或更高版本的 FMC。

- FMC 内在不支持 AnyConnect 配置文件编辑器，您必须单独配置 VPN 配置文件。在 FMC 中作为文件对象添加 VPN 配置文件和 AnyConnect VPN 软件包，它们将成为 RA VPN 配置的一部分。
- 目前不支持核心 VPN 功能之外的安全移动、网络访问管理和所有其他 AnyConnect 模块以及它们的配置文件。
- 不支持 VPN 负载均衡。
- 不支持浏览器代理。
- 不支持所有终端安全评估变体（HostScan、终端安全评估和 ISE）和基于客户端安全评估的动态访问策略。
- Firepower 威胁防御设备不会配置或部署自定义或本地化 AnyConnect 所必需的文件。
- FTD 上不支持需要 AnyConnect 客户端上自定义属性的功能，例如：桌面客户端上的延迟升级和移动客户端上的 Per-App VPN。
- 不能在 FTD 头端执行本地身份验证，因此，配置的用户不可用于远程连接，并且 FTD 不能作为证书颁发机构。此外，不支持以下身份验证功能：
  - 辅助或双重身份验证
  - 使用 SAML 2.0 的单一登录
  - TACACS、Kerberos（KCD 身份验证）和 RSA SDI
  - LDAP 授权（LDAP 属性映射）
  - RADIUS CoA

有关在 FTD 上配置和部署 AnyConnect 的详细信息，请参阅相应版本的《Firepower 管理中心配置指南（版本 6.2.1 或更高版本）》中的 *Firepower* 威胁防御远程接入 *VPN* 一章。

更新 AnyConnect 软件和配置文件

AnyConnect 可通过多种方式更新。

- AnyConnect 客户端 - 当 AnyConnect 连接到 ASA 时，AnyConnect 下载程序将检查 ASA 上是否加载了任何新软件或配置文件。AnyConnect 下载程序将这些更新下载到客户端，并将建立 VPN 隧道。
- 云更新 - Umbrella 漫游安全模块可从 Umbrella 云基础设施为所有已安装的 AnyConnect 模块提供自动更新。通过云更新，可自动从 Umbrella 云基础设施获得软件升级，且更新跟踪将取决于该软件升级，而非管理员的任何操作。默认情况下，将禁用通过云更新进行自动更新。
- ASA 或 FTD 网络门户 - 您指示用户连接到 ASA 的无客户端网络门户进行更新。FTD 仅可下载核心 VPN 模块。

- ISE - 当用户连接到 ISE 时，ISE 将使用其 AnyConnect 配置判断是否有更新的组件或新的终端安全评估要求。在授权后，网络访问设备 (NAD) 会将用户重定向到 ISE 门户，将在客户端上安装 AnyConnect 下载程序，以管理软件包提取和安装。我们建议您将部署软件包上传到 ASA 前端，并确保 AnyConnect 客户端的版本与 ASA 和 ISE 部署软件包版本相匹配。

  接收到 "在建立 VPN 隧道时，必须执行自动软件更新，但无法执行" 的消息表示配置的 ISE 策略需要更新。当本地设备上的 AnyConnect 版本比 ISE 上配置的版本更旧时，您可以选择以下选项，因为在 VPN 处于活动状态时不允许客户端更新：

  - 在带外部署 AnyConnect 更新
  - 在 ASA 和 ISE 上配置相同版本的 AnyConnect

可以允许最终用户延迟更新，并且即便您将更新载入头端，也可阻止客户端更新。

升级示例流程

必备条件

以下示例假定：

- 您已在 ISE 中创建动态授权控制列表 (DACL)，且列表已推送到 ASA。该列表使用客户端的终端安全评估状态确定何时将客户端重定向到 ISE 上的 AnyConnect 客户端调配门户。
- ISE 在 ASA 之后。

AnyConnect 已安装在客户端上

1. 用户启动 AnyConnect，提供凭证，并单击“连接”(Connect)。
2. ASA 建立与客户端的 SSL 连接，将身份验证凭证传递到 ISE，ISE 验证凭证。
3. AnyConnect 启动 AnyConnect 下载程序，该下载程序执行所有升级操作，并启动 VPN 隧道。

如果 ASA 未安装 ISE 终端安全评估，则

1. 用户浏览到任何站点时，DACL 将其重定向到 ISE 上的 AnyConnect 客户端调配门户。
2. 如果使用 Internet Explorer 浏览器，ActiveX 控件将启动 AnyConnect 下载程序。在其他浏览器中，用户下载并执行网络设置助理 (NSA)，该工具会下载并启动 AnyConnect 下载程序。
3. AnyConnect 下载程序执行在 ISE 上配置的所有 AnyConnect 升级，其中现在包括 AnyConnect ISE 终端安全评估模块。
4. 客户端上的 ISE 终端安全评估代理将启动终端安全评估。

未安装 AnyConnect

1. 用户浏览到站点，启动到 ASA 无客户端门户的连接。
2. 用户提供身份验证凭证，该凭证将传输到 ISE 并进行验证。
3. AnyConnect 下载程序由 Internet Explorer 中的 ActiveX 控件和其他浏览器中的 Java 小应用启动。
4. AnyConnect 下载程序执行在 ASA 上配置的升级，然后启动 VPN 隧道。下载程序完成。

如果 ASA 未安装 ISE 终端安全评估，则

1. 用户再次浏览到站点，然后重定向到 ISE 上的 AnyConnect 客户端调配门户。
2. 在 Internet Explorer 中，ActiveX 控件启动 AnyConnect 下载程序。在其他浏览器中，用户下载并执行网络设置助理，该工具将下载并启动 AnyConnect 下载程序。
3. AnyConnect 下载程序通过现有 VPN 隧道执行 ISE 上配置的所有升级，其中包括添加 AnyConnect ISE 终端安全评估模块。
4. ISE 终端安全评估代理启动终端安全评估。

禁用 AnyConnect 自动更新

可以通过配置和分发客户端配置文件来禁用或限制 AnyConnect 自动更新。

- 在 VPN 客户端配置文件中：
  - Auto Update 将禁用自动更新。您可以将此配置文件包括在 AnyConnect 网络部署安装中，或添加到现有的客户端安装中。您也可以允许用户切换此设置。
- 在 VPN 本地策略配置文件中：
  - 绕过下载程序阻止将 ASA 上的任何更新内容下载到客户端。
  - Update Policy 在连接到不同头端时提供对软件和配置文件更新的精细控制。

在 WebLaunch 期间提示用户下载 AnyConnect

您可以将ASA配置为提示远程用户启动网络部署，并配置一个时间段，在这个时间段内他们可以选择下载 AnyConnect 或转到无客户端入口页面。

提示用户下载AnyConnect在组策略或用户帐户中进行配置。以下步骤显示如何在组策略中启用此功能。

步骤 1 在 ASDM 中，转到**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **组策略 (Group Policies)**。

步骤 2 选择组策略，单击**编辑 (Edit)** 或**添加 (Add)** 可编辑或新增组策略。

步骤 3 在导航窗格中，选择**高级 (Advanced)** > **AnyConnect 客户端 (AnyConnect Client)** > **登录设置 (Login Settings)**。如果需要，取消选中**继承 (Inherit)** 复选框，然后选择“登录后”(Post Login) 设置。

如果您选择提示用户，请指定超时时间段并选择在“默认登录后选择”(Default Post Login Selection) 区域中该时间段过期后要采取的默认操作。

步骤 4 单击**确定 (OK)** 并确保将更改应用到组策略中，然后单击**保存 (Save)**。

允许用户延期升级

您可以强制用户通过禁用 AutoUpdate 接受 AnyConnect 更新，如禁用 AnyConnect 自动更新中所述。默认情况下，AutoUpdate 为启用状态。

也可以允许用户延迟客户端更新，直到以后设置“延期更新”(Deferred Update)。如果配置了“延期更新”(Deferred Update)，当客户端更新可用时，AnyConnect 会打开一个对话框，询问用户是希望立即更新，还是希望延迟更新。所有 Windows、Linux 和 OS X 都支持 Deferred Upgrade（延期更新）。

在 ASA 上配置延迟更新

在 ASA 上，通过添加定制属性，然后在组策略中引用和配置这些属性，可以启用延迟更新。必须创建并配置**所有**自定义属性以使用延迟升级。

向 ASA 配置添加定制属性的过程取决于所运行的 ASA/ASDM 版本。请根据您部署的 ASA/ASDM 版本，参阅 *Cisco ASA* 系列 *VPN ASDM* 配置指南或 *Cisco ASA* 系列 *VPN CLI* 配置指南，了解定制属性配置过程。

以下属性和值用于在 ASDM 中配置延迟更新：

定制属性 *	有效值	默认值	备注
DeferredUpdateAllowed	true false	False	True 可以启用延迟更新。如果延迟更新被禁用 (false)，以下设置会被忽略。
DeferredUpdateMinimumVersion	*x.x.x*	0.0.0	实现更新可延迟所必须要安装的最低 AnyConnect 版本。 此最低版本检查适用于在前端上启用的所有模块。如果启用的任意模块（包括 VPN）未安装或不符合最低版本要求，则连接不符合延迟更新条件。 如果未指定此属性，无论在终端上安装的版本如何，系统都会显示（或自动关闭）延迟提示。

定制属性 *	有效值	默认值	备注
DeferredUpdateDismissTimeout	0-300 （秒）	150 秒	延迟升级提示在自动关闭之前显示的秒数。仅当显示延迟更新提示时才应用此属性（先评估最低版本属性）。 如果此属性缺失，则禁用自动关闭功能，对话框会一直显示（如需要），直到用户作出响应。 将此属性设置为零，则允许根据以下条件强制进行自动延迟或升级： • 已安装的版本和 DeferredUpdateMinimumVersion 的值。 • DeferredUpdateDismissResponse 的值。
DeferredUpdateDismissResponse	延迟更新	更新	发生 DeferredUpdateDismissTimeout 时采取的操作。

* 定制属性值区分大小写。

在 ISE 中配置延期更新

步骤 1 遵循以下步骤进行导航：

a) 选择**策略 (Policy)** > **结果 (Results)**。

b) 展开 **Client Provisioning**。

c) 选择**资源 (Resources)**，然后单击**添加 (Add)** > **来自本地磁盘的代理资源 (Agent resources from local disk)**。

d) 上传 AnyConnect pkg 文件，然后选择**提交 (Submit)**。

步骤 2 上载您创建的任何其他 AnyConnect 资源。

步骤 3 在 **Resources** 上，使用您上传的 AnyConnect 软件包添加 **AnyConnect Configuration**。AnyConnect Configuration 具有用于配置延期更新的字段。

延期更新 GUI

下图显示当有更新可用且配置了延迟更新时用户看到的用户界面。图的右边部分显示当配置了 **DeferredUpdateDismissTimeout** 时的用户界面。

设置更新策略

更新策略概述

如果 AnyConnect 软件和配置文件更新可用且客户端允许更新，则可在连接到前端时进行更新。为 AnyConnect 更新配置前端，以便可以进行更新。VPN 本地策略文件中的更新策略设置决定了是否允许更新。

更新策略有时被称之为软件锁定。如果配置了多个前端，更新策略也称之为多域策略。

默认情况下，更新策略设置允许来自任何前端的软件和配置文件更新。请按如下方式设置更新策略参数以限制此操作：

- 通过在 **Server Name** 列表中指定头端，允许或授权特定头端更新所有 AnyConnect 软件和配置文件。

  前端服务器名可以是 FQDN 或 IP 地址。同时也可以是通配符，例如：*.example.com。

  有关更新发生方式的完整说明，请参阅以下已授权服务器更新策略行为。

- 对于所有其他未指定或未授权的前端：
  - 使用 **Allow Software Updates From Any Server** 选项，允许或拒绝 VPN 核心模块和其他可选模块的软件更新。
  - 使用 **Allow VPN Profile Updates From Any Server** 选项，允许或拒绝 VPN 配置文件更新。
  - 使用 **Allow Service Profile Updates From Any Server** 选项，允许或拒绝其他服务模块配置文件更新。
  - 使用**允许任何服务器的 ISE 终端安全评估配置文件更新 (Allow ISE Posture Profile Updates From Any Server)** 选项，允许或拒绝 ISE 终端安全评估配置文件更新。
  - **使用允许来自任何服务器的合规性模块更新 (Allow Compliance Module Updates From Any Server)** 选项，允许或拒绝合规性模块更新。

    有关更新发生方式的完整说明，请参阅以下未授权的服务器更新策略行为。

已授权服务器更新策略行为

当连接到 **Server Name** 列表中的已授权头端时，其他更新策略参数不适用并且会出现以下情况：

- 比较前端上 AnyConnect 软件包的版本与客户端版本，以确定软件是否应该更新。
  - 如果 AnyConnect 软件包的版本比客户端上的版本旧，则不进行软件更新。
  - 如果 AnyConnect 软件包的版本与客户端上的版本相同，则只下载和安装在前端上配置以供下载并且在客户端上不存在的软件模块。
  - 如果 AnyConnect 软件包的版本比客户端的版本新，则下载和安装前端上为下载配置的软件模块以及客户端上已安装的软件模块。

- 前端上的 VPN 配置文件、ISE 终端安全评估配置文件和每个服务配置文件都将与客户端上的配置文件进行比较以确定是否应更新：
  - 如果前端的配置文件与客户端的配置文件相同，则不会进行更新。
  - 如果前端的配置文件与客户端的配置文件不同，则会进行下载。

未授权的服务器更新策略行为

连接到未授权的头端时，系统将通过 **Allow ... Updates From Any Server** 选项确定 AnyConnect 的更新方式，如下所述：

- **Allow Software Updates From Any Server:**
  - 如果选中此选项，则允许对此未授权的ASA进行软件更新。根据对上述授权前端的版本比较进行更新。
  - 如果未选中此选项，则不会进行软件更新。此外，如果基于版本比较发生更新，系统将终止 VPN 连接尝试。
- **Allow VPN Profile Updates From Any Server:**
  - 如果选中此选项，则当前端的 VPN 配置文件与客户端的配置文件不同时，对 VPN 配置文件进行更新。
  - 如果未选中此选项，则不会更新 VPN 配置文件。此外，如果基于差异发生 VPN 配置文件更新，系统将终止 VPN 连接尝试。
- **Allow Service Profile Updates From Any Server:**
  - 如果选中此选项，则当前端的配置文件与客户端的配置文件不同时，对每个服务配置文件进行更新。
  - 如果未选中此选项，则不会更新服务配置文件。
- **Allow ISE Posture Profile Updates From Any Server:**
  - 如果选中此选项，则在前端 ISE 终端安全评估配置文件不同于客户端 ISE 终端安全评估配置文件时，更新 ISE 终端安全评估配置文件。
  - 如果未选中此选项，则不会更新 ISE 终端安全评估配置文件。ISE 终端安全评估代理需要具备 ISE 终端安全评估配置文件才能运行。
- **Allow Compliance Module Updates From Any Server:**
  - 如果选中此选项，则在前端合规性模块不同于客户端合规性模块时更新合规性模块。
  - 如果未选中此选项，则不更新合规性模块。ISE 终端安全评估代理需要具备合规性模块才能运行。

更新策略指南

- 通过在授权的 **Server Name** 列表中列出服务器的 IP 地址，远程用户可以使用该 IP 地址连接到头端。如果用户尝试使用 IP 地址连接，但前端被列为 FQDN，那么该尝试将被视为连接到未授权的域。
- 软件更新包括下载定制、本地化、脚本和转换。在禁止软件更新时，将不会下载这些项目。如果某些客户端不允许脚本更新，请不要依赖脚本来实施策略。
- 下载启用永远在线的 VPN 配置文件将删除客户端上的所有其他 VPN 配置文件。在决定允许或拒绝从未授权前端或非企业前端更新 VPN 配置文件时，请注意这一点。
- 如果因安装和更新策略而未能将 VPN 配置文件下载到客户端，则以下功能将不可用：

服务禁用	不受信任网络策略
证书存储区覆盖	受信任的 DNS 域
显示预连接消息	受信任 DNS 服务器
本地局域网接入	永远在线
登录前开始	强制网络门户补救
本地代理连接	脚本编写
PPP 排除	注销时保持 VPN
自动 VPN 策略	需要设备锁定
受信任的网络策略	自动服务器选择

- 在 Windows 中，下载程序将创建一个单独的文本日志 (UpdateHistory.log) 来记录下载历史信息。此日志包含更新时间、更新客户端的 ASA、更新的模块以及升级前后安装的版本。此日志文件存储于：

  `%ALLUSERESPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Logs` 目录。
- 您必须重新启动 AnyConnect 服务才能选择本地策略文件中的任何更改。

更新策略示例

此示例显示了客户端上的 AnyConnect 版本不同于各 ASA 前端时客户端的更新行为。

假定 VPN 本地策略 XML 文件中的更新策略如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
xmlns=http://schemas.xmlsoap.org/encoding/
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
<FipsMode>false</FipsMode>
<BypassDownloader>false</BypassDownloader><RestrictWebLaunch>false</RestrictWebLaunch>
<StrictCertificateTrust>false</StrictCertificateTrust>
```

```
<RestrictPreferenceCaching>false</RestrictPreferenceCaching>
<RestrictTunnelProtocols>false</RestrictTunnelProtocols>
<UpdatePolicy>
<AllowSoftwareUpdatesFromAnyServer>false</AllowSoftwareUpdatesFromAnyServer>
<AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>
<AllowVPNProfileUpdatesFromAnyServer>false</AllowVPNProfileUpdatesFromAnyServer>
<AllowManagementVPNProfileUpdatesFromAnyServer>true</AllowManagementVPNProfileUpdatesFromAnyServer>
<AllowISEProfileUpdatesFromAnyServer>true</AllowISEProfileUpdatesFromAnyServer>
<AllowServiceProfileUpdatesFromAnyServer>false</AllowServiceProfileUpdatesFromAnyServer>
<AllowScriptUpdatesFromAnyServer>true</AllowScriptUpdatesFromAnyServer>
<AllowHelpUpdatesFromAnyServer>true</AllowHelpUpdatesFromAnyServer>
<AllowResourceUpdatesFromAnyServer>true</AllowResourceUpdatesFromAnyServer>
<AllowLocalizationUpdatesFromAnyServer>true</AllowLocalizationUpdatesFromAnyServer>
<AuthorizedServerList>
    <ServerName>seattle.example.com</ServerName>
    <ServerName>newyork.example.com</ServerName>
</AuthorizedServerList>
</UpdatePolicy>
</AnyConnectLocalPolicy>
```

有以下 ASA 前端配置：

ASA 前端	加载的 AnyConnect 软件包	要下载的模块
seattle.example.com	版本 4.7.01076	VPN、网络访问管理器
newyork.example.com	版本 4.7.03052	VPN、网络访问管理器
raleigh.example.com	版本 4.7.04056	VPN、终端安全评估

当客户端当前运行 AnyConnect VPN 和网络访问管理器模块时，可能出现以下更新序列：

- 客户端连接到 seattle.example.com，这是一个采用相同版本的 AnyConnect 来配置的授权服务器。如果 VPN 和网络访问管理器配置文件可供下载，且不同于客户端上的 VPN 和配置文件，则也会被下载。
- 客户端随后连接到 newyork.example.com，这是一个采用较新版本的 AnyConnect 来配置的授权 ASA。VPN 和网络访问管理器模块会进行升级。若配置文件可供下载且不同于客户端上的配置文件，则也会被下载。
- 客户端随后连接到 raleigh.example.com，这是一个未授权的 ASA。即使需要进行软件更新并且也有软件更新可用，但由于策略决定了不允许版本升级，因此无法进行更新。连接终止。

AnyConnect 参考信息

本地计算机上用户首选项文件的位置

AnyConnect 将某些配置文件设置存储在用户计算机上的用户首选项文件和全局首选项文件中。AnyConnect 使用本地文件配置客户端 GUI 上“首选项”(Preferences) 选项卡中用户可控制的设置并显示有关最新连接的信息，如用户、组和主机。

AnyConnect 使用全局文件来配置登录之前发生的操作，例如 Start Before Login 和 AutoConnect On Start。

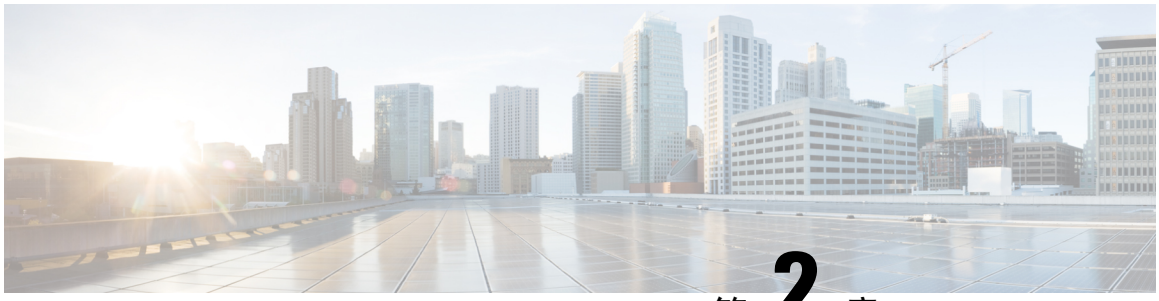
下表显示客户端计算机上首选项文件的文件名和安装路径：

操作系统	类型	文件和路径
Windows	用户	C:\Users\username\AppData\Local\Cisco\ Cisco AnyConnect VPN Client \ preferences.xml
	全局	C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\ preferences_global.xml
macOS	用户	/Users/username/.anyconnect
	全局	/opt/cisco/anyconnect/.anyconnect_global
Linux	用户	/home/username/.anyconnect
	全局	/opt/cisco/anyconnect/.anyconnect_global

AnyConnect 使用的端口

下表列出了每个协议的 Cisco AnyConnect Secure Mobility Client 使用的端口。

协议	思科 AnyConnect 客户端端口
TLS (SSL)	TCP 443
SSL 重定向	TCP 80（可选）
DTLS	UDP 443（可选，但强烈推荐）
IPsec/IKEv2	UDP 500、UDP 4500



第 2 章

定制和本地化 AnyConnect 客户端和安装程序

修改 AnyConnect 安装行为

指南

- Web 部署使用 AnyConnect Web 启动，后者是无客户端 SSL 门户的一部分。可以定制无客户端 SSL 门户，但不能定制门户的 AnyConnect 部分。例如，不能定制“启动 AnyConnect”(Start AnyConnect) 按钮。

禁用客户体验反馈

默认情况下，已启用客户体验反馈模块。此模块向思科提供有关客户已启用和正在使用的功能和模块的匿名信息。此信息让我们可以深入了解用户体验，以便思科可以持续改进质量、可靠性、性能和用户体验。

要手动禁用客户体验反馈模块，请使用独立配置文件编辑器创建一个CustomerExperience_Feedback.xml文件。必须停止 AnyConnect 服务，将该文件命名为 CustomerExperience_Feedback.xml，然后将其放在 C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback\ 目录中。如果该文件是通过禁用标志集创建的，则可将此文件手动部署到 AnyConnect。要检查结果，请

打开 AnyConnect 的“关于”(About) 菜单，然后验证并确保客户体验反馈模块未在“已安装模块”(Installed Module) 部分列出。

可使用以下方法禁用客户体验反馈模块：

- 客户体验反馈模块客户端配置文件 - 取消选中“启用客户体验反馈服务”(Enable Customer Experience Feedback Service)，并分发此配置文件。
- MST 文件 - 从 anyconnect-vpn-transforms-X.X.xxxxx.zip 中提取 anyconnect-win-disable-customer-experience-feedback.mst 文件。

修改安装行为 (Windows)

使用以下 Windows 安装程序属性来修改 AnyConnect 安装行为。在 ISO 映像中，安装程序 setup.hta 是 HTML 文件并且可以编辑。

注释 AnyConnect 不支持 Windows Installer ADVERTISE 模式。

- 命令行参数 - 一个或多个属性作为参数传递到命令行安装程序 msiexec。此方法用于预部署，网络部署不支持此方法。
- 安装程序转换 - 可以使用转换修改安装程序属性表。多种工具可用于创建转换。一个常用工具是 Microsoft Orca。Orca 工具是 Microsoft Windows Installer 软件开发套件 (SDK) 的一部分，包含在 Microsoft Windows SDK 内。要获取 Windows SDK，请浏览至 http://msdn.microsoft.com，然后搜索与您的 Windows 版本对应的 SDK 并下载。

  转换仅可用于预部署。（当下载程序调用安装程序时，只有思科签署的转换才能用于网络部署。）您可通过带外方法应用您自己的转换，但详情已经超出本指南的范围。

限制

AnyConnect 卸载提示不可定制。

用于定制客户端安装的 Windows 安装程序属性

以下 Windows 安装程序属性可定制 AnyConnect 安装。请注意，您还可以使用 Microsoft 支持的很多其他 Windows 安装程序属性。

- Resetting the System MTU - 当 VPN 安装程序属性 (RESET_ADAPTER_MTU) 设置为 1 时，安装程序会将所有 Windows 网络适配器 MTU 设置重置为默认值。必须重新启动系统，更改方可生效。
- 设置 Windows 锁定 - 思科建议为设备上的最终用户授予有限的Cisco AnyConnect Secure Mobility Client权限。如果最终用户拥有额外的权限，安装程序可提供锁定功能，防止用户和本地管理员关闭或停止 AnyConnect 服务。您还可以使用服务密码通过命令提示符来停止服务。

适用于 VPN、网络访问管理器、Network Visibility Module 和 Umbrella 漫游安全模块的 MSI 安装程序支持一个公用属性 (LOCKDOWN)。当 LOCKDOWN 设置为非零值时，终端设备上的用户或本地管理员无法控制与该安装程序关联的 Windows 服务。我们建议您使用我们提供的示例转换来设置此属性，并将转换应用于您希望锁定的每个 MSI 安装程序。您可以从Cisco AnyConnect Secure Mobility Client软件下载页面下载示例转换。

如果部署核心客户端以及一个或多个可选模块，则必须对每个安装程序应用锁定属性。此操作为单向操作，无法删除，除非您重新安装产品。

注释 AMP 启用程序安装程序与 VPN 安装程序配对使用。

- 开启 ActiveX 控件 - 在默认情况下，早期版本的 AnyConnect 在预部署 VPN 软件包时会安装 VPN WebLaunch ActiveX 控件。从 AnyConnect 3.1 开始，默认情况下将关闭 VPN ActiveX 控件安装。此更改旨在确保默认配置最为安全。

  在预部署 AnyConnect 客户端和可选模块时，如果您需要将 VPN ActiveX 控件与 AnyConnect 一同安装，则您必须使用 NOINSTALLACTIVEX=0 选项和 msiexec 或转换。

- Hiding AnyConnect from the Add/Remove Program List - 可从用户 Windows Control Panel 中的 Add/Remove Program 列表中隐藏已安装的 AnyConnect 模块。向安装程序传送 ARPSYSTEMCOMPONENT=1 可阻止该模块显示在已安装程序的列表中。

  我们建议您使用我们提供的示例转换来设置此属性，从而将转换应用于您希望隐藏的每个模块的每个 MSI 安装程序。您可以从Cisco AnyConnect Secure Mobility Client软件下载页面下载示例转换。

AnyConnect 模块的 Windows 安装程序属性

下表提供 MSI 安装命令行调用和配置文件部署位置的示例。

已安装的模块	命令和日志文件
没有 VPN 功能的 AnyConnect 核心客户端 （在安装独立模块时使用）	msiexec /package anyconnect-win-*version*-predeploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* anyconnect-win-*version*-predeploy-k9-install-datetimestamp.log
有 VPN 功能的 AnyConnect 核心客户端	msiexec /package anyconnect-win-*version*-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-predeploy-k9-install-datetimestamp.log

已安装的模块	命令和日志文件
客户体验反馈	msiexec /package anyconnect-win-*version*-predeploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* anyconnect-win-*version*-predeploy-k9-install-datetimestamp.log
诊断和报告工具 (DART)	msiexec /package anyconnect-win-*version*-dart-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-dart-predeploy-k9-install-datetimestamp.log
SBL	msiexec /package anyconnect-win-*version*-gina-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-gina-predeploy-k9-install-datetimestamp.log
网络访问管理器	msiexec /package anyconnect-win-*version*-nam-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-nam-predeploy-k9-install-datetimestamp.log
状态	msiexec /package anyconnect-win-*version*-posture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-posture-predeploy-k9-install-datetimestamp.log
ISE 终端安全评估	msiexec /package anyconnect-win-*version*-iseposture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-*version*-iseposture-predeploy-k9-install-datetimestamp.log
AMP 启用程序	msiexec /package anyconnect-win-*version*-amp-predeploy-k9.msi /norestart/ passive /lvx* anyconnect-win-*version*-amp-predeploy-k9-install-datetimestamp.log
网络可视性模块	msiexec /package anyconnect-win-*version*-nvm-predeploy-k9.msi /norestart/ passive /lvx* anyconnect-win-*version*-nvm-predeploy-k9-install-datetimestamp.log
Umbrella 漫游安全模块	msiexec /package anyconnect-win-*version*-umbrella-predeploy-k9.msi/norestart/ passive /lvx* anyconnect-win-*version*-predeploy-k9-install-datetimestamp.log

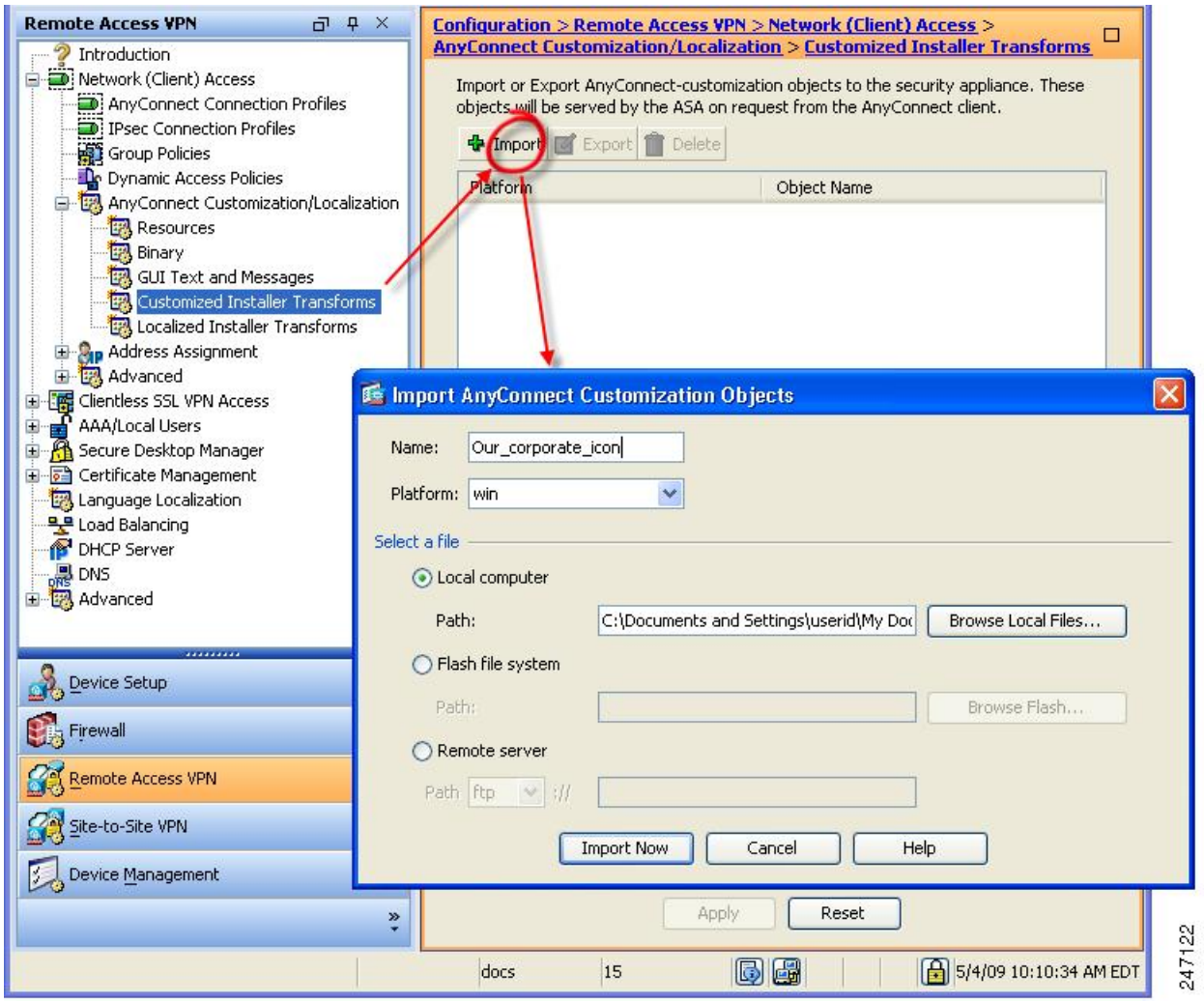
将定制安装程序转换导入自适应安全设备

将思科提供的 Windows 转换导入自适应安全设备让您可以将其用于网络部署。

步骤 1 在 ASDM 中，转到 **配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **AnyConnect 定制/本地化 (AnyConnect Customization/Localization)** > **定制安装程序转换 (Customized Installer Transforms)**。

步骤 2 单击**导入 (Import)**。

系统会显示“导入 AnyConnect 定制对象”(Import AnyConnect Customization Objects) 窗口：



步骤 3 输入要导入的文件名。转换文件的名称决定了安装程序转换文件该应用于哪个模块。您可以使用以下语法来全局或按模块应用转换：

a) *_name*.mst：应用于所有安装程序

b) <moduleid>*_name*.mst：应用于单个模块安装程序

c) *name*.mst：仅应用于 VPN 安装程序

步骤 4 选择平台，并指定要导入的文件。单击**立即导入 (Import Now)**。此文件会立即显示在安装程序转换表中。

本地化 AnyConnect 安装程序屏幕

您可以翻译 AnyConnect 安装程序显示的消息。ASA 使用转换功能来翻译安装程序显示的消息。该转换会更改安装，但会保持原始安全签名的 MSI 不变。这些转换仅翻译安装程序屏幕，而不翻译客户端 GUI 屏幕。

注释 AnyConnect 的每个版本都包括本地化转换，管理员可在上传含有新软件的 AnyConnect 软件包时将转换上传到自适应安全设备。如果您使用我们的本地化转换，请确保在上传新的 AnyConnect 软件包时用 cisco.com 的最新版本更新这些转换。

我们目前提供 30 种语言转换。这些转换在 cisco.com 的 AnyConnect 软件下载页面以下面的 .zip 文件形式提供：

```
anyconnect-win-<VERSION>-webdeploy-k9-lang.zip
```

在此文件中，<VERSION> 是 AnyConnect 的版本（例如 4.3.xxxxx）。

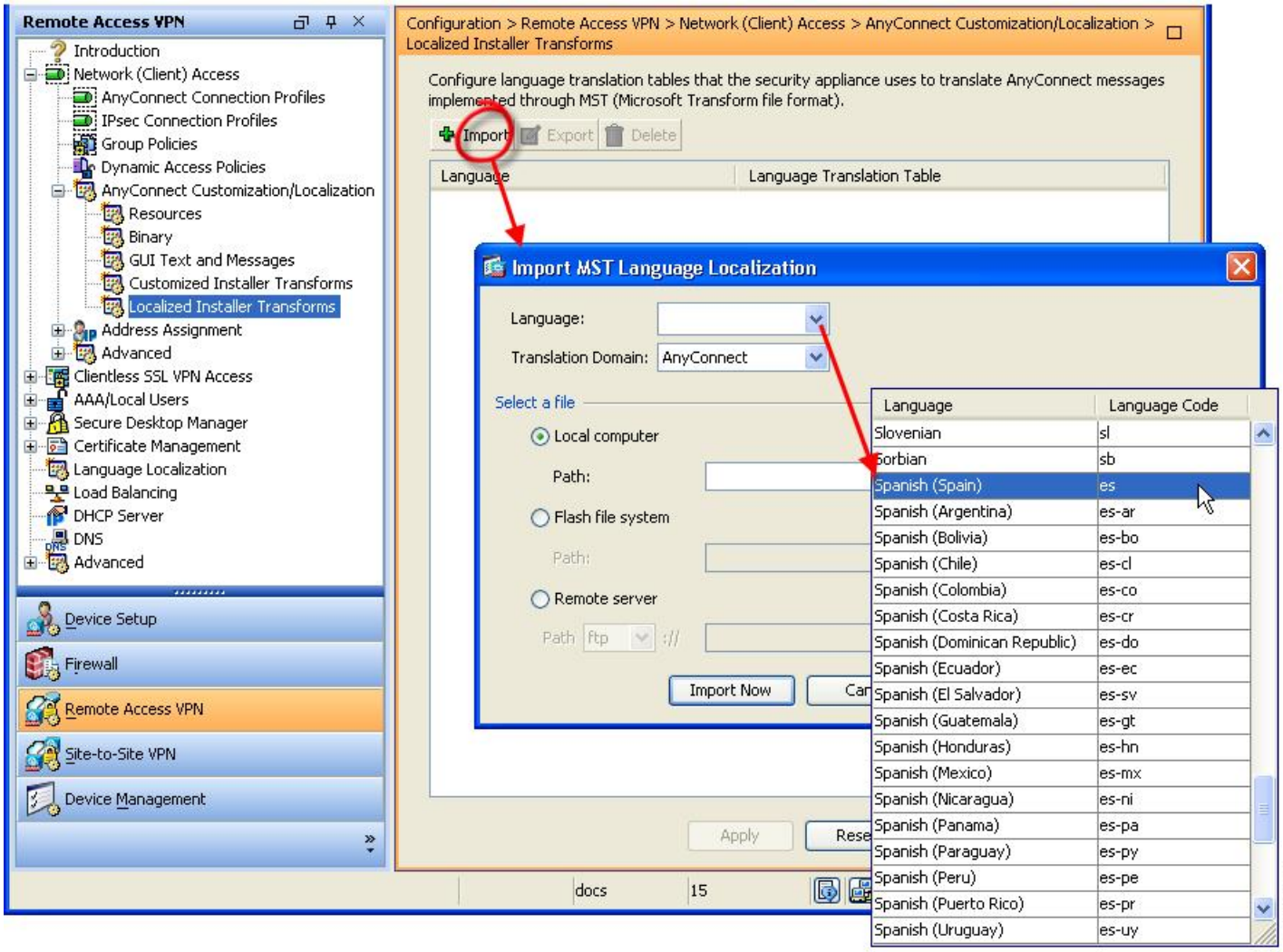
存档包含用于可用翻译的转换（.mst 文件）。如果需要为远程用户提供的语言不是我们提供的 30 种语言之一，您可以创建您自己的转换并将其作为新语言导入 ASA。使用 Microsoft 的数据库编辑器 Orca，可以修改现有安装以及新文件。Orca 是 Microsoft Windows 安装程序软件开发套件 (SDK) 的一部分，包含在 Microsoft Windows SDK 内。

将本地化的安装程序转换导入自适应安全设备

以下过程显示如何使用 ASDM 将转换导入 ASA。

步骤 1 在 ASDM 中，转到 **配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **AnyConnect 定制/本地化 (AnyConnect Customization/Localization)** > **本地化的安装程序转换 (Localized Installer Transforms)**。

步骤 2 单击**导入 (Import)**。系统将打开“导入 MST 语言本地化”(Import MST Language Localization) 窗口：



步骤 3 单击**语言 (Language)** 下拉列表，选择用于此转换的一种语言（和行业认可的缩写）。如果您手动输入缩写，请确保使用浏览器和操作系统识别的缩写。

步骤 4 单击**立即导入 (Import Now)**。
将显示已成功导入表格的提示消息。

步骤 5 单击**应用 (Apply)** 保存更改。

在此过程中我们将语言指定为西班牙语 (ES)。下图显示在 Languages 列表中的用于 AnyConnect 的西班牙语新转换。

修改安装行为 (macOS)

AnyConnect 安装程序无法本地化。该安装程序使用的字符串来自 macOS 安装应用，而不是 AnyConnect 安装程序。

注释 您不能改变用户在安装程序 UI 中看到的可选模块选择。要更改安装程序 UI 中的默认可选模块选择，需要编辑安装程序，这样做将使签名失效。

使用 ACTransform.xml 在 macOS 上自定义安装程序行为

由于 macOS 没有提供任何标准方法来自定义 .pkg 行为，所以我们创建了 ACTransforms.xml。使用安装程序定位此 XML 文件时，安装程序读取本文件，然后运行安装。您必须将文件置于与安装程序相关的特定位置。安装程序按以下顺序搜索以查看是否找到修改：

1. 在与 .pkg 安装程序文件相同的目录内的“Profile”目录中。
2. 在装载的磁盘映像卷的根目录中的“Profile”目录中。
3. 在装载的磁盘映像卷的根目录中的“Profile”目录中。

XML 文件格式如下：

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

例如，macOS ACTransforms.xml 属性是 DisableVPN，用于创建 NVM 的“独立”部署。ACTransforms.xml 在 DMG 文件所在的 Profiles 目录中。

禁用客户体验反馈模块

默认情况下，已启用客户体验反馈模块。要在 macOS 上关闭此功能，请执行以下操作：

步骤 1 使用磁盘实用程序或 hdiutil 将 dmg 软件包从只读转换为读/写。例如：

```
hdiutil convert anyconnect-macosx-i386-ver-k9.dmg -format UDRW -o anyconnect-macosx-i386-ver-k9-rw.dmg
```

步骤 2 编辑 ACTransforms.xml 并设置或添加以下值（如果尚未设置）。

```
<DisableCustomerExperienceFeedback>false</DisableCustomerExperienceFeedback>
```

修改安装行为 (Linux)

使用 ACTransform.xml 在 Linux 上定制安装程序行为

没有为 Linux 提供定制 .pkg 行为的标准方式，所以我们创建了 ACTransforms.xml。使用安装程序定位此 XML 文件时，安装程序读取本文件，然后运行安装。您必须将文件置于与安装程序相关的特定位置。安装程序按以下顺序搜索以查看是否找到修改：

- 在与 .pkg 安装程序文件相同的目录内的“Profile”目录中
- 在装载的磁盘映像卷的根目录中的“Profile”目录中
- 在与 .dmg 文件相同的目录内的“Profile”目录中

预部署软件包中的 Profiles 目录内的 XML 文件 ACTransforms.xml 的格式如下：

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

启用 DSCP 预留

您可以设置一个自定义属性，从而只对 DTLS 连接控制 Windows 或 OS X 平台上的差分服务代码点 (DSCP)。DSCP 预留允许设备优先处理延迟敏感型流量。路由器考虑是否已对此进行了设置，并对优先级流量进行标记以提高出站连接质量。

该自定义属性类型为 DSCPPreservationAllowed，有效值为 True 或 False。

注释 默认情况下，AnyConnect 执行 DSCP 预留 (True)。要禁用该功能，请将头端上的自定义属性值设置为 false，并重新启动连接。

在 ASDM 中，此功能在以下位置配置：**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（客户端访问）(Network (Client) Access) > 组策略 (Group Policies) > 添加/编辑 (Add/Edit) > 高级 (Advanced) > AnyConnect 客户端 (AnyConnect Client) > 自定义属性 (Custom Attributes)**。有关配置过程，请参阅相应版本的思科 ASA 系列 VPN 配置指南中的启用 *DSCP* 预留部分。

设置公共 DHCP 服务器路由

在配置 Tunnel All Networks 的情况下，为了让本地 DHCP 流量能够不受阻碍地传输，AnyConnect 在 AnyConnect 客户端连接时将向本地 DHCP 服务器添加特定路由。为了防止此路由出现数据泄露，AnyConnect 还对主机设备的局域网适配器应用隐式过滤器，在该路由中阻止除 DHCP 流量外的所有流量。如果您连接到外部接口，并在连接建立后使用本地 DHCP 服务器，将创建到该服务器的特定路由，指向 NIC 而非虚拟适配器。如果同一台服务器上还运行着其他服务（如 WINS 或 DNS），则此路由将在 VPN 会话建立后中断这些服务。

在 Windows 上，通过设置组策略自定义属性，可对公共 DHCP 服务器路由的创建进行控制。no-dhcp-server-route 自定义属性必须存在并设置为 true，才能避免在建立隧道后创建公共 DHCP 服务器路由。

在 ASDM 中，此功能在以下位置配置：**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（客户端访问）(Network (Client) Access) > 组策略 (Group Policies) > 添加/编辑 (Add/Edit) > 高级 (Advanced) > AnyConnect 客户端 (AnyConnect Client) > 自定义属性 (Custom Attributes)**。有关配置过程，请参阅相应版本的思科 ASA 系列 VPN 配置指南。

定制 AnyConnect GUI 文本和消息

自适应安全设备 (ASA) 使用转换表转换 AnyConnect 显示的用户消息。转换表是具有转换消息文本字符串的文本文件。您可以使用 ASDM 或转换（用于 Windows）编辑现有消息或添加其他语言。

以下 Windows 本地化转换示例在 www.cisco.com 上提供：

- 用于 Windows 平台预部署软件包的语言本地化转换文件
- 用于 Windows 平台网络部署软件包的语言本地化转换文件

Windows 的 AnyConnect 软件包文件包含用于 AnyConnect 消息的默认英语模板。当您在 ASA 中加载 AnyConnect 软件包时，ASA 会自动导入此文件。此模板包含 AnyConnect 软件中消息字符串的最新更改。您可以使用为其他语言创建新的转换表，也可以导入 www.cisco.com 上提供的以下转换表之一（请参阅将转换表导入自适应安全设备，第 52 页）：

- 中文（简体）
- 中文（繁体）
- 捷克语
- 荷兰语
- 法语
- 法语（加拿大）
- 德语
- 匈牙利语

- 意大利语
- 日语
- 韩语
- 波兰语
- 葡萄牙语（巴西）
- 俄文
- 西班牙文（拉美）

以下各节介绍所需语言不可用或您希望进一步定制导入转换表时转换 GUI 文本和消息的过程。

- 添加或编辑 AnyConnect 文本和消息。您可以按照以下任一方式添加或编辑文件来更改一个或多个消息 ID 的消息文本，从而更改消息文件：
  - 在打开的对话框中键入对文本的更改。
  - 将打开的对话框中的文本复制到文本编辑器，进行更改，然后粘贴回对话框。
- 将转换表导入自适应安全设备，第 52 页。您可以通过单击“保存到文件”(Save to File) 来导出消息文件，进行编辑，并将其导入回 ASDM。

在 ASA 上更新转换表后，直到客户端重新启动并成功建立另一个连接，才会应用更新后的消息。

注释 如果没有从 ASA 部署客户端和使用诸如 Altiris Agent 的公司软件部署系统，您可以采用诸如 Gettext 的目录实用程序手动将 AnyConnect 转换表 (anyconnect.po) 转换为 .mo 文件并将 .mo 文件安装到客户端计算机的相应文件夹中。有关详细信息，请参阅为企业部署创建消息目录。

指南和限制

AnyConnect 并不完全符合所有国际化要求，但以下内容除外：

- 日期/时间格式并不总是遵循区域设置要求。
- 不支持从右到左的语言。
- 由于硬编码字段的长度要求，有些字符串在 UI 中会截断。
- 一些硬编码英语字符串保持如下：
  - 更新时的状态消息。
  - 不受信任的服务器消息。
  - 延期更新消息。

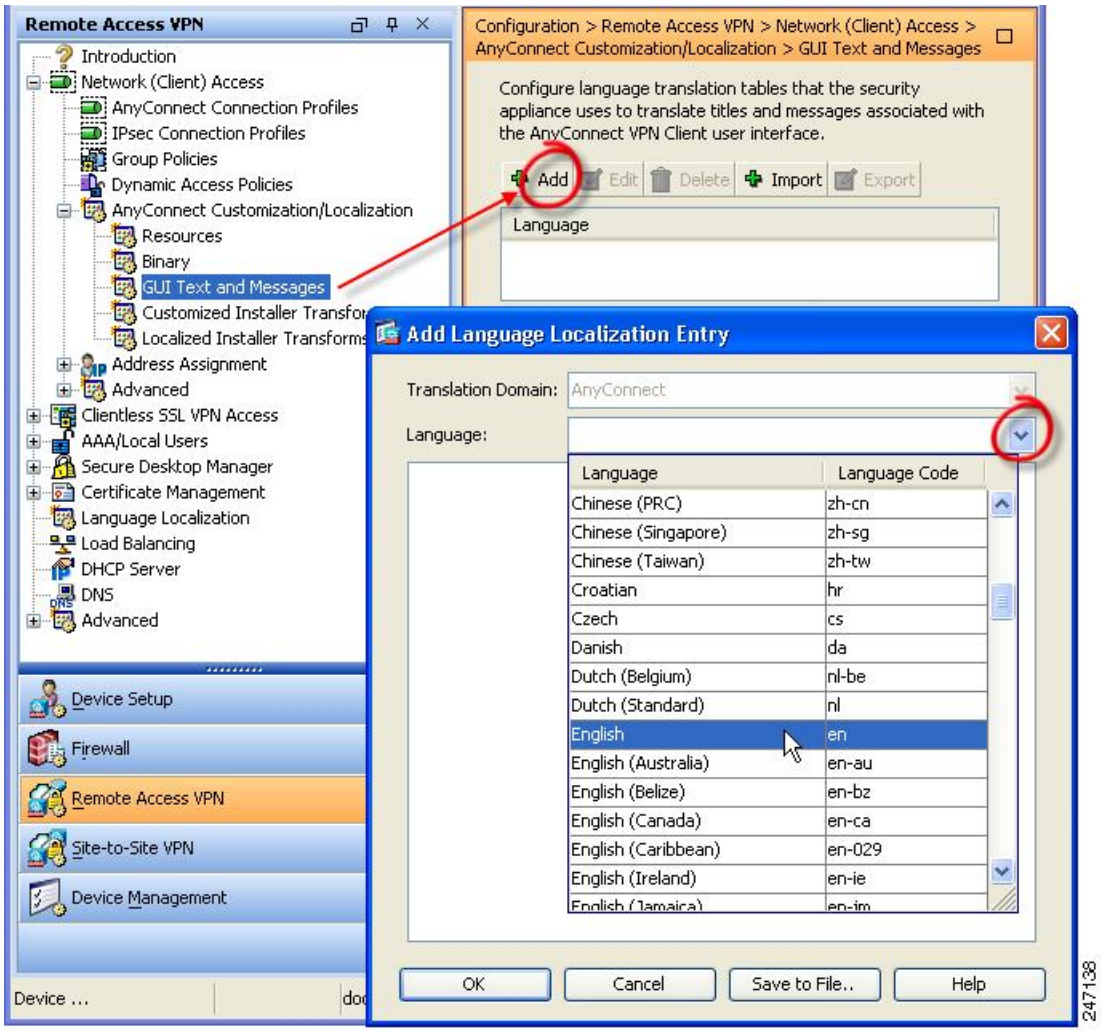
添加或编辑 AnyConnect 文本和消息

您可以通过添加或编辑英语转换表并且更改一条或多条消息 ID 的消息文本，来更改 AnyConnect GUI 上显示的英文消息。打开消息文件后，您可通过以下方式编辑：

- 在打开的对话框中键入对文本的更改。
- 将打开的对话框中的文本复制到文本编辑器，进行更改，然后粘贴回对话框。
- 单击“保存到文件”(Save to File)、编辑文件并将其导入到 ASDM，以导出消息文件。

步骤 1 在 ASDM 中，转到 **配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **AnyConnect 定制/本地化 (AnyConnect Customization/Localization)** > **GUI 文本和消息 (GUI Text and Messages)**。

步骤 2 单击**添加 (Add)**。系统将显示“添加语言本地化条目”(Add Language Localization Entry) 窗口。

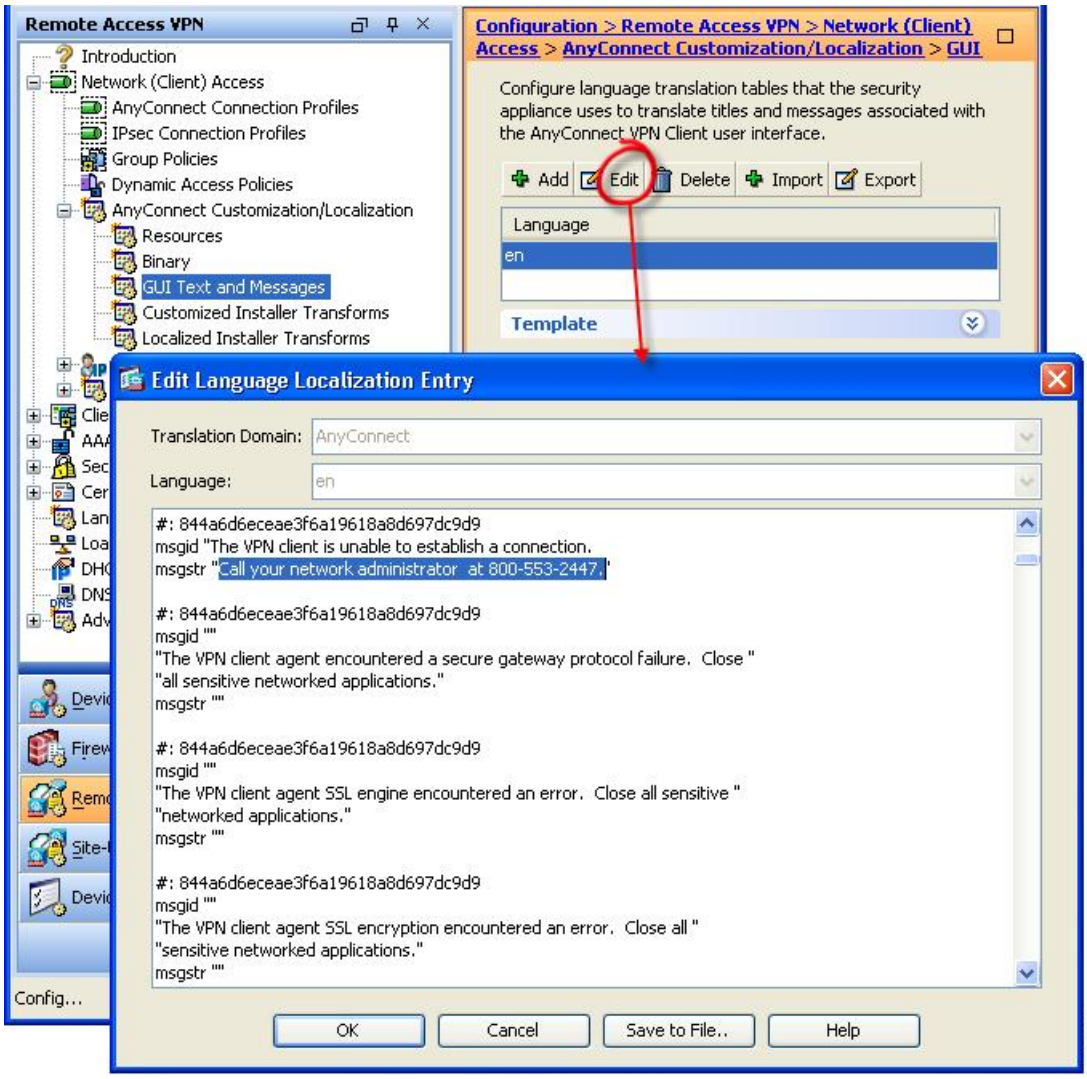


步骤 3 单击“语言”(Language) 下拉列表，然后指定语言为英语 (en)。英语转换表显示在窗格的语言列表中。

步骤 4 单击**编辑 (Edit)** 开始编辑消息。

系统将显示“编辑语言本地化条目”(Edit Language Localization Entry) 窗口。msgid 的引号之间的文本是客户端显示的默认英语文本，不能更改。msgstr 字符串包含客户端用于替换 msgid 中默认文本的文本。在 msgstr 的引号之间插入您自己的文本。

在以下示例中，我们插入“Call your network administrator at 800-553-2447”。



步骤 5 单击**确定 (OK)**，然后单击**应用 (Apply)** 以保存更改。

将转换表导入自适应安全设备

步骤 1 从 www.cisco.com 下载所需的转换表。

步骤 2 在 ASDM 中，转到 **配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **AnyConnect 定制/本地化 (AnyConnect Customization/Localization)** > **GUI 文本和消息 (GUI Text and Messages)**。

步骤 3 单击**导入 (Import)**。系统会显示“导入语言本地化条目”(Import Language Localization Entry) 窗口。

步骤 4 从下拉列表中选择适合的语言。

步骤 5 指定从何处导入转换表。

步骤 6 单击**立即导入 (Import Now)**。即可将此转换表部署至 AnyConnect 客户端，并将其用作首选语言。本地化将在 AnyConnect 重新启动并连接后应用。

注释 对于在非移动设备上运行的 AnyConnect，即使没有使用思科安全桌面，也必须将思科安全桌面转换表导入自适应安全设备，这样 HostScan 消息才会进行本地化。

为企业部署创建消息目录

如果没有将客户端与 ASA 一起部署，且正在使用企业软件部署系统（例如 Altiris Agent），则可以使用实用程序（例如 Gettext）将 AnyConnect 转换表手动转换为消息目录。将表格从 .po 文件转换为 .mo 文件，之后将文件置于客户端计算机上相应的文件夹内。

注释 GetText 和 PoeEdit 是第三方软件应用。AnyConnect GUI 定制的推荐方法是从 ASA 获取默认的 .mo 文件，然后根据任何部署到客户端的需要编辑该文件。使用默认 .mo 可以避免第三方应用（例如 GetText 和 PoeEdit）导致的潜在转换问题。

Gettext 是来自 GNU 项目的实用程序并在命令窗口中运行。有关详细信息，请参阅 GNU 网站 gnu.org。还可以使用基于 GUI 的实用程序（该程序使用 Gettext），例如 Poedit。poedit.net 上提供了此软件。此过程使用 Gettext 来创建消息目录：

AnyConnect 消息模板目录

AnyConnect 消息模板位于以下为每个操作系统列出的文件夹中：

注释 `\l10n` 目录是如下所列的每个目录路径的一部分。目录名称拼写：小写 l ("el")、1、0、小写 n。

- 对于 Windows - `<DriveLetter>:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\l10n\<LANGUAGE-CODE>\LC_MESSAGES`

- 对于 macOS 和 Linux - `/opt/cisco/anyconnect/l10n/<LANGUAGE-CODE>/LC_MESSAGES`

步骤 1 从 http://www.gnu.org/software/gettext/ 下载 Gettext 实用程序并将 Gettext 安装在您用于管理的计算机（不是远程用户计算机）上。

步骤 2 在已安装 AnyConnect 的计算机上检索 AnyConnect 消息模板 AnyConnect.po 的副本。

步骤 3 根据需要，编辑 AnyConnect.po 文件（使用 notepad.exe 或任何明文文本编辑器）来更改字符串。

步骤 4 运行 Gettext 消息文件编译器以基于 .po 文件创建 .mo 文件：

msgfmt -o AnyConnect.mo AnyConnect.po

步骤 5 将 .mo 文件副本置于用户计算机上正确的消息模板目录下。

将新消息合并到 ASA 上的定制转换表中

新用户消息将添加到 AnyConnect 的某些版本中。为启用这些新消息的转换，新消息字符串会添加到与最新客户端映像一起打包的转换模板中。如果您已基于以前的客户端附带的模板创建了转换表，新消息不会自动向远程用户显示。您必须将最新模板与您的转换表合并以确保转换表包含这些新消息。

可使用免费的第三方工具执行合并。来自 GNU 项目的 Gettext 实用程序可用于 Windows，并可在命令窗口中运行。有关详细信息，请参阅 GNU 网站 gnu.org。还可以使用基于 GUI 的实用程序（该程序使用 Gettext），例如 Poedit。poedit.net 上提供了此软件。以下过程涵盖了这两种方法。

注释 此过程假设您已将最新的 AnyConnect 映像软件包载入 ASA 中。除非您执行此操作，否则模板无法导出。

步骤 1 从**远程访问 VPN (Remote Access VPN)** > **语言本地化 (Language Localization)** > **模板 (Templates)**导出最新的 AnyConnect 转换模板。导出的模板文件名为 `AnyConnect.pot`。此文件名确保 msgmerge.exe 程序将此文件识别为消息目录模板。

步骤 2 合并 AnyConnect 模板与转换表。

如果使用的是适用于 Windows 的 Gettext 实用程序，打开命令提示符窗口并运行以下命令。该命令会合并 AnyConnect 转换表 (.po) 和模板 (.pot)，从而创建新的 `AnyConnect_merged.po` 文件：

```
msgmerge -o AnyConnect_merged.po AnyConnect.po AnyConnect.pot
```

以下示例显示命令的结果：

```
C:\Program Files\GnuWin32\bin> msgmerge -o AnyConnect_merged.po AnyConnect.po AnyConnect.pot
..................................... done.
```

如果使用 Poedit，则首先打开 AnyConnect.po 文件，转到 **文件 (File) > 打开 (Open) > <AnyConnect.po>**。然后将其与模板合并，从 POT 文件 <AnyConnect.pot> 转到 **Catalog > Update**。Poedit 将在 Update Summary 窗口显示新字符串和模糊字符串。保存文件，在下一步骤中将导入此文件。

步骤 3 将已合并的转换表导入**远程接入 VPN** > **语言本地化**。单击**导入 (Import)**，指定语言，然后选择 **AnyConnect** 作为转换域。将要导入的文件指定为 `AnyConnect_merged.po`。

在客户端上选择 Windows 的默认语言

当远程用户连接到 ASA 并下载客户端时，AnyConnect 会检测计算机的首选语言并通过检测指定系统区域设置应用相应的转换表。

在 Windows 上查看或更改指定的系统区域设置：

步骤 1 导航到**控制面板** > **区域和语言**对话框。如果按类别查看控制面板，请选择**时钟、区域和语言时钟** > **更改显示语言**。

步骤 2 指定语言/区域设置，并指定应使用这些设置作为所有用户帐户的默认设置。

注释 如果未指定位置，AnyConnect 将默认使用该语言。例如，如果未找到“fr-ca”目录，AnyConnect 将检查是否存在“fr”目录。您无需更改显示语言、位置或键盘即可查看转换。

为 AnyConnect GUI 创建定制图标和徽标

本节中的各表列出了可针对各操作系统替换的 AnyConnect 文件。表中的图像被 AnyConnect VPN 客户端和网络访问管理器模块所使用。

限制

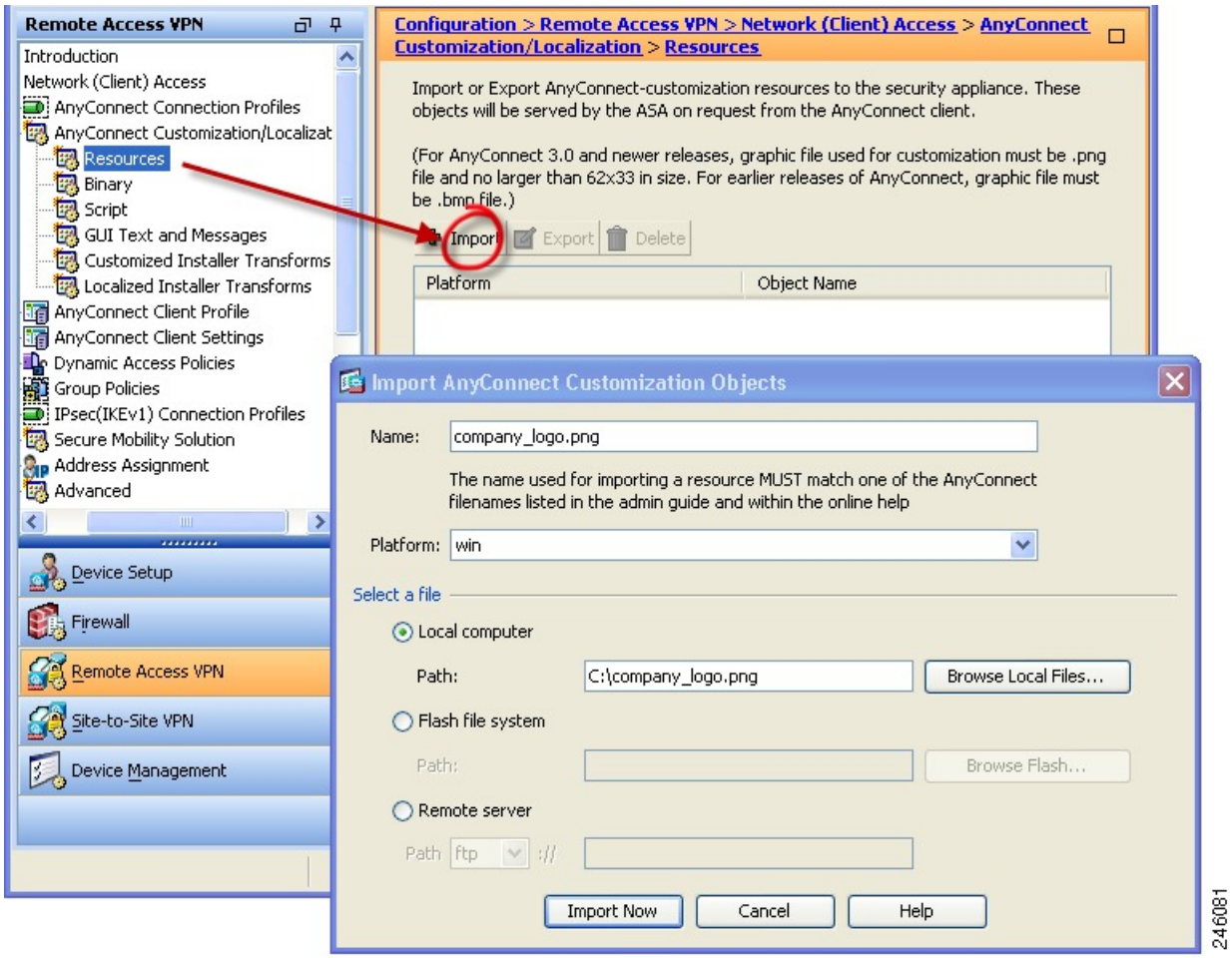
- 定制组件的文件名必须与 AnyConnect GUI 上使用的文件名一致。文件名因操作系统而有所不同，并且在 macOS 和 Linux 中区分大小写。例如，如果要替换 Windows 客户端的公司徽标，必须将您的公司徽标导入为 company_logo.png。如果以其他文件名将其导入，则 AnyConnect 安装程序不会更改组件。但是，如果您部署自己的可执行文件来定制 GUI，则该可执行文件可以使用任何文件名调用资源文件。
- 如果导入图像作为资源文件（如 company_logo.bmp），导入的图像将定制 AnyConnect，直至您重新导入另一个使用相同文件名的图像。例如，如果将 company_logo.bmp 替换为定制图像，然后删除该图像，客户端会继续显示该图像，直至导入相同文件名的新图像（或原始思科徽标图像）为止。

更换 AnyConnect GUI 组件

可通过将您自己的定制文件导入到安全设备来定制 AnyConnect，该安全设备在客户端部署新文件。

步骤 1 在 ASDM 中，转到 **配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **AnyConnect 定制/本地化 (AnyConnect Customization/Localization)** > **资源 (Resources)**。

步骤 2 单击**导入 (Import)**。**Import AnyConnect Customization Objects** 窗口随即显示。



步骤 3 输入要导入的文件名。

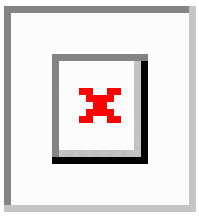
步骤 4 选择平台，并指定要导入的文件。单击**立即导入 (Import Now)**。现在，文件显示在对象列表中。

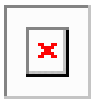
Windows 的 AnyConnect 图标和徽标

Windows 的所有文件位于：

```
%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res\
```

注释 %PROGRAMFILES% 指相同名称的环境变量。在大多数 Windows 安装中，这是 `C:\Program Files`。

Windows 安装中的文件名和说明。	图像尺寸（像素，长 x 高）和类型
about.png “高级”(Advanced) 对话框右上角的“关于”(About) 按钮。 大小不可调整。 	24 x 24 PNG
about_hover.png “高级”(Advanced) 对话框右上角的“关于”(About) 按钮。 大小不可调整。 	24 x 24 PNG
app_logo.png 128 x 128 是最大大小。如果自定义文件不是该大小，则在应用中将其调整为 128 x 128。如果比例不同，则会将其拉伸。 	128 x 128 PNG
attention.ico 系统托盘图标警告用户需要注意或交互的情况。例如，有关用户凭证的对话框。 大小不可调整。 	16 x 16 ICO

Windows 安装中的文件名和说明。	图像尺寸（像素，长 **x** 高）和类型
company_logo.png 托盘浮出控件左上角和“高级”(Advanced) 对话框中显示的公司徽标。 最大大小为 97 x 58。如果自定义文件不是该大小，则其在应用中会调整为 97 x 58。如果比例不同，则会将其拉伸。 	97 x 58（最大） PNG
company_logo_alt.png About 对话框右下角显示的公司徽标。 最大大小为 97 x 58。如果自定义文件不是该大小，则其在应用中会调整为 97 x 58。如果比例不同，则会将其拉伸。 	97 x 58 PNG

Windows 安装中的文件名和说明。	图像尺寸（像素，长 x 高）和类型
cues_bg.jpg 托盘浮出控件、“高级”(Advanced) 窗口和“关于”(About) 对话框的背景图像。 因为图像未进行拉伸，因此使用过小的替换图像会导致出现黑色区域。 	1260 x 1024 JPEG
error.ico 系统托盘图标警告用户有一个或多个组件出现严重错误。 大小不可调整。	16 x 16 ICO
neutral.ico 表示客户端组件运行正常的系统托盘图标。 大小不可调整。	16 x 16 ICO

Windows 安装中的文件名和说明。	图像尺寸（像素，长 x 高）和类型
transition_1.ico 系统托盘图标，它与 transition_2.ico 和 transition_3.ico 一同显示，表示一个或多个客户端组件在不同状态间过渡（例如 VPN 连接或网络访问管理器连接时）。3 个图标文件连续显示，看起来好像单个图标从左至右跳动。 大小不可调整。 	16 x 16 ICO
transition_2.ico 系统托盘图标，它与 transition_1.ico 和 transition_3.ico 一同显示，表示一个或多个客户端组件在不同状态间过渡（例如 VPN 连接或网络访问管理器连接时）。3 个图标文件连续显示，看起来好像单个图标从左至右跳动。 大小不可调整。 	16 x 16 ICO
transition_3.ico 系统托盘图标，它与 transition_1.ico 和 transition_2.ico 一同显示，表示一个或多个客户端组件在不同状态间过渡（例如 VPN 连接或网络访问管理器连接时）。3 个图标文件连续显示，看起来好像单个图标从左至右跳动。 大小不可调整。 	16 x 16 ICO
vpn_connected.ico 表示 VPN 已连接的系统托盘图标。 大小不可调整。 	16 x 16 ICO

Linux 的 AnyConnect 图标和徽标

Linux 的所有文件位于：

```
/opt/cisco/anyconnect/resources/
```

下表列出了您可替换的文件以及受影响的客户端 GUI 区域。

Linux 安装中的文件名和说明	图像尺寸（像素，长 x 高）和类型
company-logo.png 出现在用户界面各个选项卡上的公司徽标。 对于 AnyConnect 3.0 及更高版本，使用大小不超过 62x33 像素的 PNG 图像。 	142 x 92 PNG
CVCabout.png “关于”(About) 选项卡上显示的图标。 	16 x 16 PNG
cvc-connect.png “连接”(Connect) 按钮旁和“连接”(Connection) 选项卡上显示的图标。 	16 x 16 PNG
CVCdisconnect.png “连接”(Connection) 按钮旁显示的图标。 	16 x 16 PNG
CVCinfo.png “统计”(Statistics) 选项卡上显示的图标。 	16 x 16 PNG
systray_connected.png 客户端连接时显示的托盘图标。 	16 x 16 PNG
systray_notconnected.png 客户端未连接时显示的托盘图标。 	16 x 16 PNG
systray_disconnecting.png 客户端断开连接时显示的托盘图标。 	16 x 16 PNG

Linux 安装中的文件名和说明	图像尺寸（像素，长 x 高）和类型
systray_quarantined.png 客户端隔离时显示的托盘图标。 	16x16 PNG
systray_reconnecting.png 客户端重新连接时显示的托盘图标。 	16 x 16 PNG
vpnui48.png 主程序图标。 	48 x 48 PNG

macOS 的 AnyConnect 图标和徽标

目前不支持在 macOS 上使用 GUI 资源自定义的 AnyConnect 图标和徽标。

创建并上传 AnyConnect 客户端帮助文件

要向 AnyConnect 用户提供帮助，请创建有关您站点的附带说明的帮助文件，并将其载入自适应安全设备上。当用户通过 AnyConnect 连接时，AnyConnect 将下载帮助文件，并在 AnyConnect 用户界面显示帮助图标。当用户单击帮助图标时，浏览器将打开帮助文件。支持 PDF 和 HTML 文件。

步骤 1 创建名为 `help_AnyConnect.html` 的 HTML 文件。

步骤 2 在 ASDM 中，转到**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **AnyConnect 定制/本地化 (AnyConnect Customization/Localization)** > **二进制文件 (Binary)**。

步骤 3 导入 **help_AnyConnect.xxx** 文件。支持的格式如下：PDF、HTML、HTM 和 MHT。

步骤 4 在 PC 上，启动 AnyConnect 并连接到自适应安全设备。将帮助文件下载至客户端 PC。
您应该看到帮助图标已自动添加至 UI。

步骤 5 单击帮助图标可在浏览器中打开帮助文件。

如果帮助图标未出现，请查看帮助目录以查看 AnyConnect 下载程序是否能检索帮助文件。

下载程序将删除文件名的“help_”部分，因此您应该在以下目录之一看到 AnyConnect.html（具体因操作系统而异）：

- Windows - `C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Help`

- macOS - `/opt/cisco/anyconnect/help`

编写和部署脚本

发生以下事件时，您可以通过 AnyConnect 下载和运行脚本：

- 与安全设备建立新的客户端 VPN 会话。我们将此事件触发的脚本称为 *OnConnect* 脚本，因为该脚本需要此文件名前缀。
- 用安全设备终止客户端 VPN 会话时。我们将此事件触发的脚本称为 *OnDisconnect* 脚本，因为该脚本需要此文件名前缀。

值得信赖的网络检测发起的建立新客户端 VPN 会话将触发 OnConnect 脚本（假设满足运行脚本的要求），但网络中断后重新连接永久性 VPN 会话不会触发 OnConnect 脚本。

介绍此功能使用方法的某些示例包括：

- VPN 连接后刷新组策略。
- VPN 连接后映射网络驱动器，断开连接后取消映射。
- VPN 连接后登录到服务，断开连接后注销服务。

AnyConnect 支持在 WebLaunch 和独立启动期间启动脚本。

这些说明假定您了解如何编写脚本，并了解如何从目标终端的命令行运行脚本以进行脚本测试。

注释 AnyConnect 软件下载站点提供了某些示例脚本。查看时，请注意这些只是示例脚本。它们可能无法满足本地计算机运行这些脚本的要求，也可能在未针对网络和用户需求进行定制之前无法使用。思科不支持示例脚本或客户编写的脚本。

脚本要求和限制

请注意脚本有以下要求和限制：

- 支持的脚本数量 - AnyConnect 仅运行一个 OnConnect 脚本和一个 OnDisconnect 脚本。但这些脚本可启动其他脚本。
- 文件格式 - AnyConnect 通过文件名识别 OnConnect 脚本和 onDisconnect 脚本。它查找名称以 OnConnect 或 OnDisconnect 开头的文件，并忽略文件扩展名。AnyConnect 将执行找到的第一个前缀匹配的脚本。AnyConnect 可识别解释型脚本（例如 VBS、Perl 或 Bash）或可执行文件。
- 脚本语言 - 客户端不要求脚本以特定语言编写，但要求在客户端计算机上安装可运行脚本的应用。因此，为了保证客户端可以启动脚本，脚本必须能够从命令行运行。

- Windows 安全环境对脚本的限制 - 在 Microsoft Windows 中，AnyConnect 仅在用户登录 Windows 并建立 VPN 会话后方可启动脚本。因此，用户的安全环境施加的限制适用于这些脚本。脚本只能执行用户有权调用的功能。AnyConnect 将在 Windows 执行脚本期间隐藏 cmd 窗口，因此用户无法出于测试目的在 .bat 文件中执行显示消息的脚本。
- 启用脚本 - 默认情况下，客户端不会启动脚本。应使用 AnyConnect 配置文件 EnableScripting 参数来启用脚本。执行该操作时，客户端不要求提供脚本。
- 客户端 GUI 终止 - 客户端 GUI 终止不一定会终止 VPN 会话。OnDisconnect 脚本在会话终止后运行。
- 在 64 位 Windows 中运行脚本 - AnyConnect 客户端是 32 位应用。在 64 位 Windows 版本中运行时，AnyConnect 将使用 cmd.exe 的 32 位版本。

  由于 32 位 cmd.exe 缺乏某些 64 位 cmd.exe 支持的命令，因此某些脚本可能会在尝试运行不支持的命令时停止执行，或部分运行后停止。例如，32 位版本的 Windows 7 可能无法理解 64 位 cmd.exe 支持的 msg 命令（位于 %WINDIR%\SysWOW64 中）。

  因此，在创建脚本时，请使用 32 位 cmd.exe 支持的命令。

编写、测试和部署脚本

在目标操作系统上编写和测试您的脚本。如果脚本无法从本地操作系统的命令行正常运行，则 AnyConnect 也无法正常运行该脚本。

步骤 1 编写和测试您的脚本。

步骤 2 选择部署脚本的方式：

- 使用 ASDM 将脚本作为二进制文件导入 ASA。

  转到**网络 (客户端) 接入** > **AnyConnect 自定义/本地化** > **脚本**。

  如果您使用 ASDM 6.3 版或更高版本，ASA 会在您的文件名中添加前缀 scripts_ 和前缀 OnConnect 或 OnDisconnect，以将该文件识别为脚本。当客户端连接时，安全设备会将脚本下载到远程计算机的相应目标目录中，删除 scripts_ 前缀，并保留 OnConnect 或 OnDisconnect 前缀。例如，如果您导入脚本 myscript.bat，则脚本将在安全设备中显示为 scripts_OnConnect_myscript.bat。在远程计算机上，脚本显示为 OnConnect_myscript.bat。

  如果您使用的 ASDM 版本低于 6.3，则您必须导入具有以下前缀的脚本：

  - scripts_OnConnect
  - scripts_OnDisconnect

    为确保脚本能够稳定运行，请将所有 ASA 配置为部署相同的脚本。如果您要修改或替换脚本，请使用与早期版本相同的名称，并将替换脚本分配到用户可能连接的所有 ASA。当用户连接时，新脚本将覆盖同名脚本。

- 使用企业软件部署系统手动将脚本部署到 VPN 终端。

如果您使用此方法，请使用以下脚本文件名前缀：

- OnConnect
- OnDisconnect

在以下目录中安装脚本：

表 *5:* 规定的脚本位置

操作系统	目录
Microsoft Windows	%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Script
Linux （在 Linux 中，为用户、组和其他类型的文件分配执行权限。）	/opt/cisco/anyconnect
macOS	/opt/cisco/anyconnect/script

为脚本配置 AnyConnect 配置文件

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **首选项（部分 2）(Preferences [Part 2])**。

步骤 2 选中**启用脚本功能 (Enable Scripting)**。客户端在连接或断开 VPN 连接时启动脚本。

步骤 3 选中**用户可控制 (User Controllable)** 使用户可以启用或禁用 On Connect 和 OnDisconnect 脚本的运行。

步骤 4 选中**终止下一个事件上的脚本 (Terminate Script On Next Event)**，可在过渡到另一个可编写脚本的事件时使客户端可以终止运行脚本流程。例如，在 AnyConnect 启动新 VPN 会话时，如果 VPN 会话结束并终止运行 OnDisconnect 脚本，则客户端会终止运行 On Connect 脚本。在 Microsoft Windows 上，客户端也会终止 On Connect 或 OnDisconnect 脚本启动的所有脚本及其所有脚本派生项。在 macOS 和 Linux 上，客户端只会终止 OnConnect 或 OnDisconnect 脚本，它不会终止子脚本。

步骤 5 选中**SBL 建立会话时启用 OnConnect 脚本 (Enable Post SBL On Connect Script)**（默认情况下启用）可在 SBL 建立 VPN 会话时使客户端启动 On Connect 脚本（如果有）。

注释 请务必将客户端配置文件添加到 ASA 组策略，以将其下载到 VPN 终端。

脚本故障排除

如果脚本无法运行，按如下所述尝试解决问题：

步骤 1 确保脚本有 `OnConnect` 或 `OnDisconnect` 前缀名称。编写、测试和部署脚本显示每个操作系统所需的脚本目录。

步骤 2 尝试从命令行运行脚本。如果无法从命令行运行脚本，客户端便无法运行脚本。如果脚本在命令行运行失败，请确保已安装运行脚本的应用，并尝试在操作系统上重写脚本。

步骤 3 验证 VPN 终端上的脚本目录中仅有一个 OnConnect 脚本和一个 OnDisconnect 脚本。如果客户端从 ASA 下载 OnConnect 脚本，然后下载与另一个 ASA 的文件名后缀不同的另一个 OnConnect 脚本，则客户端可能不会运行您打算运行的脚本。如果脚本路径包含多个 OnConnect 或 OnDisconnect 脚本，而且您正在使用 ASA 部署脚本，则删除脚本目录的内容并重新建立 VPN 会话。如果脚本路径包含多个 OnConnect 或 OnDisconnect 脚本，而且您采用手动部署方法，则删除不需要的脚本并重新建立 VPN 会话。

步骤 4 如果操作系统是 Linux，请确保脚本文件的权限已设置为执行。

步骤 5 确保客户端配置文件已启用脚本功能。

使用 AnyConnect API 编写和部署定制应用

对于 Windows、Linux 和 macOS 计算机，您可以使用 AnyConnect API 开发自己的可执行用户界面 (UI)。通过替换 AnyConnect 二进制文件部署您的 UI。

下表列出了不同操作系统的客户端可执行文件的文件名。

客户端操作系统	客户端 GUI 文件	客户端 CLI 文件
Windows	vpnui.exe	vpncli.exe
Linux	vpnui	vpn
macOS	ASA 部署不支持。但是，您可以为使用其他方法（例如 Altiris Agent）替换客户端 GUI 的 macOS 部署可执行文件。	vpn

可执行文件能够调用您导入 ASA 的任何资源文件，例如徽标图像。部署自己的可执行文件时，您可以对资源文件使用任意文件名。

限制

- 无法从自适应安全设备部署更新的 AnyConnect 软件。如果您在自适应安全设备上放置了更新版本的 AnyConnect 软件包，AnyConnect 客户端将下载更新，可替换定制 UI。您必须处理定制客户端以及相关 AnyConnect 软件的分发问题。尽管 ASDM 允许您上传二进制文件以替换 AnyConnect 客户端，但在使用定制应用时不支持此部署功能。
- 如果您部署网络安全或网络访问管理器，请使用Cisco AnyConnect Secure Mobility Client GUI。
- 不支持登录前启动。

使用 AnyConnect CLI 命令

思科 AnyConnect VPN 客户端为更喜欢输入客户端命令而不喜欢使用图形用户界面的用户提供了命令行界面 (CLI)。以下几个小节介绍了如何启动 CLI 命令提示符，以及可以通过该 CLI 使用的命令：

- 启动客户端 CLI 提示，第 66 页
- 使用客户端 CLI 命令，第 66 页
- 在 ASA 终止会话时阻止 Windows 弹出消息，第 68 页

注释 在 Windows 和 macOS 中，同一下载程序会被用于 VPN UI 或 CLI 连接中的配置文件更新。在 Linux 中，VPN UI 的下载程序可以显示警告和弹出窗口，例如我们在连接或下载配置文件或其他组件时经常看到的不受信任证书警告。但是，VPN CLI 的第二个 Linux 下载程序无法显示此类弹出窗口和警告，并且您会收到连接失败消息，这是预期行为。

启动客户端 CLI 提示

要启动 CLI 命令提示符：

- (Windows) 在 Windows 文件夹 C:/Program Files/Cisco/Cisco AnyConnect Secure Mobility Client 中找到文件 *vpncli.exe*。双击 vpncli.exe。
- （Linux 和 macOS）在文件夹 /opt/cisco/anyconnect/bin/ 中找到文件 *vpn*。执行文件 *vpn*。

使用客户端 CLI 命令

如果您在交互模式下运行 CLI，则它将提供自己的提示。您还可以使用命令行。

- connect *IP address or alias* - 客户端将建立与特定 ASA 的连接
- disconnect - 客户端将关闭先前建立的连接
- stats - 显示关于已建立的连接的统计信息
- quit - 退出 CLI 交互模式
- exit - 退出 CLI 交互模式

以下示例显示了用户通过命令行建立和终止连接：

Windows 的 ISE 安全评估代理

```
connect 209.165.200.224
```

建立与地址为209.165.200.224的安全设备的连接。在与请求的主机联系后，AnyConnect客户端将显示用户所属的群组，并询问用户的用户名和密码。如果您已制定显示可选横幅，则用户必须对该横幅作出响应。默认响应为 n，这将终止连接尝试。例如：

```
VPN > connect 209.165.200.224
>>contacting host (209.165.200.224) for login information...
>>Please enter your username and password.
Group: testgroup
Username: testuser
Password: ********
>>notice: Please respond to banner.
VPN>
STOP! Please read. Scheduled system maintenance will occur tonight from 1:00-2:00 AM for
one hour.
The system will not be available during that time.

accept? [y/n] y
>> notice: Authentication succeeded. Checking for updates...
>> state: Connecting
>> notice: Establishing connection to 209.165.200.224.
>> State: Connected
>> notice: VPN session established.
VPN>
```

stats

显示当前连接的统计信息；例如：

```
VPN > stats
[Tunnel information]

Time Connected: 01:17:33
Client Address: 192.168.23.45
Server Address: 209.165.200.224

[Tunnel Details]

Tunneling Mode: All traffic
Protocol: DTLS
Protocol Cipher: RSA_AES_256_SHA1
Protocol Compression: None

[Data Transfer]

Bytes (sent/received): 1950410/23861719
Packets (sent/received): 18346/28851
Bypassed (outbound/inbound): 0/0
Discarded (outbound/inbound): 0/0

[Secure Routes]

Network Subnet
0.0.0.0 0.0.0.0
VPN>
```

“断开连接”(disconnect)

关闭先前建立的连接；例如：

```
VPN > disconnect
>> state: Disconnecting
>> state: Disconnected
>> notice: VPN session ended.
VPN>
```

quit 或 exit

其中任何一个命令都将退出 CLI 交互模式；例如：

```
quit
goodbye
>>state: Disconnected
```

Linux 或 macOS

```
/opt/cisco/anyconnect/bin/vpn connect 1.2.3.4
```

建立与地址为 1.2.3.4 的 ASA 的连接

```
/opt/cisco/anyconnect/bin/vpn connect some_asa_alias
```

通过读取配置文件建立与 ASA 的连接，并查找别名 *some_asa_alias* 以便找到其地址

```
/opt/cisco/anyconnect/bin/vpn stats
```

显示关于该 vpn 连接的统计信息

```
/opt/cisco/anyconnect/bin/vpn disconnect
```

断开该 vpn 会话（如果存在）

在 ASA 终止会话时阻止 Windows 弹出消息

如果您通过从 ASA 发布会话重置命令来终止 AnyConnect 会话，将向终端用户显示以下 Windows 弹出消息：

```
The secure gateway has terminated the vpn connection. The following message was received
for the gateway: Administrator Reset
```

您可能不希望显示此消息（例如，在使用 CLI 命令发起 VPN 隧道时）。您可以通过在客户端连接后重新启动客户端 CLI 来阻止显示此消息。下面的示例显示了当您进行此操作时 CLI 的输出结果：

```
C:/Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client>vpncli
Cisco AnyConnect Secure Mobility Client (version 4.x).
Copyright (c) 2016 Cisco Systems, Inc.
All Rights Reserved.
>> state: Connected
>> state: Connected
>> notice: Connected to asa.cisco.com.
>> notice: Connected to asa.cisco.com.
>> registered with local VPN subsystem.
>> state: Connected
>> notice: Connected to asa.cisco.com.
>> state: Disconnecting
>> notice: Disconnect in progress, please wait...
>> state: Disconnected
>> notice: On a trusted network.
>> error: The secure gateway has terminated the VPN connection.
The following message was received from the secure gateway: Administrator Reset
VPN>
```

另外，您还可以在 Windows 注册表中，在位于以下位置的终端设备上创建一个名为 SuppressModalDialogs 的 32 位双精度值。客户端将检查该名称，但会忽略其值：

- 64 位 Windows：

HKEY_LOCAL_MACHINE/SOFTWARE\Wow6432Node\Cisco\ Cisco AnyConnect Secure Mobility Client

- 32 位 Windows：

  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client

准备 AnyConnect 定制和本地化进行 ISE 部署

准备 AnyConnect 本地化捆绑包

AnyConnect 本地化捆绑包是包含用于本地化 AnyConnect 的转换表文件和安装程序转换文件的压缩文件。此压缩文件是 ISE AnyConnect 资源的一部分，该资源用于从 ISE 向用户部署 AnyConnect。此压缩文件的内容由 AnyConnect 部署中您支持的语言进行定义，如此过程中所述。

开始之前

ISE 要求在其 AnyConnect 本地化捆绑包中有经过编译的二进制转换表。在 Gettext 中有两种文件格式：用于进行编辑的文本 .po 格式，和在运行时使用的经过编译的二进制 .mo 格式。可使用 Gettext 工具 msgfmt 完成编译。从 http://www.gnu.org/software/gettext/ 下载 Gettext 实用程序并在您用于管理的本地计算机（不是远程用户计算机）上安装 Gettext。

步骤 1 获取并准备 AnyConnect 部署使用的转换表文件。

a) 在 www.cisco.com 上的Cisco AnyConnect Secure Mobility Client Software Download 页面上，下载并打开 `AnyConnect-translations-`（日期）`.zip` 文件。

   此压缩文件包含思科提供的所有语言转换的 *.po 文件。

b) （可选） 查找您已为自己的环境定制或创建的任何其他转换表文件（*.po 文件）。

c) 运行 Gettext 消息文件编译器以从您正使用的各个 *.po 文件创建 *.mo 文件：

   `msgfmt -o AnyConnect.mo AnyConnect.po`

步骤 2 汇编 AnyConnect 部署使用的转换表文件。

a) 在本地计算机的工作区中创建名为 `l10n` 的目录。

b) 为要包含的各个语言在 `l10n` 下创建目录，以语言代码命名。

   例如，`fr-ch` 代表法语（加拿大）。

c) 将要包含的各个编译转换表放入适当命名的目录中。

   请勿将任何 *.po 文件放在经过编译的转换表中。仅应将 *.mo 文件放在此文件中。

目录结构与以下类似，其中包括法语（加拿大）、希伯来语和日语的转换表：

```
l10n\fr-ch\AnyConnect.mo
    \he\AnyConnect.mo
    \ja\AnyConnect.mo
```

步骤 3 （仅适用于 Windows）获取并准备 AnyConnect 部署所使用的语言本地化转换文件。

a) 在 www.cisco.com 上的Cisco AnyConnect Secure Mobility Client 的软件下载页，下载并打开包含语言本地化转换文件的压缩文件，该文件会将转换应用于安装程序屏幕。

压缩文件名为 `anyconnect-win-（版本）-webdeploy-k9-lang.zip`。

注释 语言本地化文件的版本必须与您的环境中使用的 AnyConnect 版本一致。当升级到 AnyConnect 的新版本时，还必须将本地化捆绑包中使用的语言本地化文件升级到同一版本。

b) 找到您为自己的环境定制或创建的所有语言本地化转换文件。

步骤 4 （仅适用于 Windows）汇编 AnyConnect 部署使用的语言本地化文件。

a) 在本地计算机的同一工作区中创建名为 `mst` 的目录。

b) 为要包含的各个语言在 `mst` 下创建目录，以语言代码命名。

例如，`fr-ch` 代表法语（加拿大）。

c) 将要包含的各个语言本地化文件放入适当命名的目录中。

现在，您的目录结构与以下结构类似：

```
l10n\fr-ch\AnyConnect.mo
    \he\AnyConnect.mo
    \ja\AnyConnect.mo
mst\fr-ch\AnyConnect_fr-ca.mst
   \he\AnyConnect_he.mst
   \ja\AnyConnect_ja.mst
```

步骤 5 使用标准压缩实用程序将此目录结构压缩到适当命名的文件中，例如 `AnyConnect-Localization-Bundle-（版本）.zip`，以创建 AnyConnect 本地化捆绑包。

下一步做什么

将 AnyConnect 本地化捆绑包作为 ISE AnyConnect 资源（用于向用户部署 AnyConnect）的一部分上传到 ISE。

准备 AnyConnect 定制捆绑包

AnyConnect 定制捆绑包是包含定制 AnyConnect GUI 资源、定制帮助文件、VPN 脚本和安装程序转换的压缩文件。此压缩文件是 ISE AnyConnect 资源的一部分，该资源用于从 ISE 向用户部署 AnyConnect。它的目录结构如下：

```
win\resource\
   \binary
   \transform
mac-intel\resource
         \binary
         \transform
```

自定义的 AnyConnect 组件包含在 Windows 和 macOS 平台的 `resource`、`binary` 和 `transform` 子目录中，具体如下所示：

- 每个 `resource` 子目录都包含该平台的所有定制 AnyConnect GUI 组件。

要创建这些资源，请参阅为 AnyConnect GUI 创建定制图标和徽标，第 54 页。

- 每个 `binary` 子目录都包含该平台的定制帮助文件和 VPN 脚本。
  - 要创建 AnyConnect 帮助文件，请参阅创建并上传 AnyConnect 客户端帮助文件，第 61 页。
  - 要创建 VPN 脚本，请参阅编写和部署脚本，第 62 页。
- 每个 `transform` 子目录都包含该平台的安装程序转换。
  - 要创建 Windows 定制安装程序转换，请参阅 修改安装行为 (Windows)，第 40 页
  - 要创建 macOS 安装程序转换，请参阅 使用 ACTransform.xml 在 macOS 上自定义安装程序行为，第 46 页

开始之前

准备 AnyConnect 定制捆绑包之前，先创建所有必要的定制组件。

步骤 1 在本地计算机的工作区创建所述目录结构。

步骤 2 在 `resources` 目录下存放各个平台的定制 AnyConnect GUI 文件。确认文件均适当命名，且图标和徽标的大小合适。

步骤 3 在 `binary` 目录下存放定制 `help_AnyConnect.html` 文件。

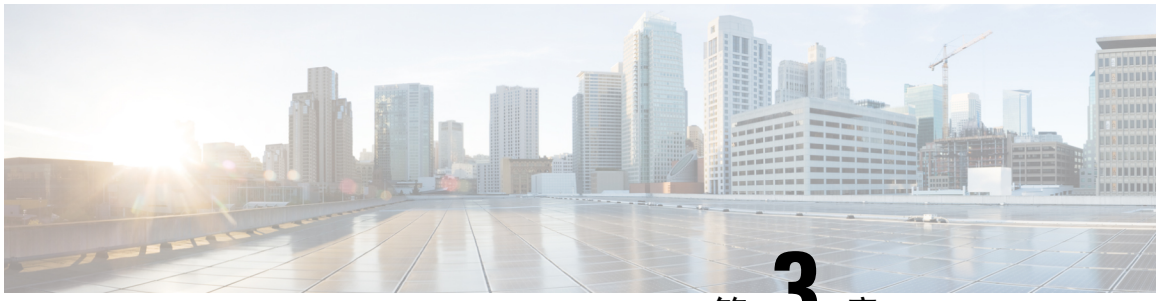
步骤 4 在 `binary` 目录下存放 VPN `OnConnect` 和 `OnDisconnect` 脚本及其调用的任何其他脚本。

步骤 5 在 `transform` 目录下存放特定于平台的安装程序转换。

步骤 6 使用标准压缩实用程序将此目录结构压缩到适当命名的文件中，例如 `AnyConnect-Customization-Bundle.zip`，以创建 AnyConnect 定制捆绑包。

下一步做什么

将 AnyConnect 定制捆绑包作为 ISE AnyConnect 资源（用于向用户部署 AnyConnect）的一部分上传到 ISE。



第 3 章

AnyConnect 配置文件编辑器

关于配置文件编辑器

Cisco AnyConnect Secure Mobility Client 软件包包含适用于所有操作系统的配置文件编辑器。在 ASA 上加载 AnyConnect 客户端映像时，ASDM 会激活配置文件编辑器。您可从本地或闪存上传客户端配置文件。

如果加载多个 AnyConnect 软件包，ASDM 会激活来自最新的 AnyConnect 软件包的客户端配置文件编辑器。此方法可确保编辑器显示所加载的最新 AnyConnect 以及早期版本客户端的功能。

还有在 Windows 上运行的独立配置文件编辑器。

从 ASDM 添加新配置文件

注释 在创建客户端配置文件之前，必须先上传客户端映像。

配置文件按照管理员定义的最终用户要求和终端上的身份验证策略部署为 AnyConnect 的一部分，使预配置的网络配置文件可供最终用户使用。使用配置文件编辑器创建并配置一个或多个配置文件。AnyConnect 将配置文件编辑器作为 ASDM 的一部分，并且作为独立的 Windows 程序。

要从 ASDM 向 ASA 添加新的客户端配置文件，请执行以下操作：

步骤 1 打开 ASDM，并选择**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **AnyConnect 客户端配置文件 (AnyConnect Client Profile)**。

步骤 2 单击**添加 (Add)**。

步骤 3 输入配置文件名称。

步骤 4 从“配置文件用途”(Profile Usage) 下拉列表中选择要为其创建配置文件的模块。

步骤 5 （可选）在“配置文件位置”(Profile Location) 字段中，单击**浏览闪存 (Browse Flash)**，并选择 ASA 上 XML 文件的设备文件路径。

步骤 6 （可选）如果使用独立编辑器创建了配置文件，请单击**上传 (Upload)** 以使用该配置文件定义。

步骤 7 （可选）从下拉列表中选择 AnyConnect 组策略。

步骤 8 单击**确定 (OK)**。

AnyConnect VPN 配置文件

AnyConnect 配置文件中启用了Cisco AnyConnect Secure Mobility Client功能。这些配置文件包含核心客户端 VPN 功能和可选客户端模块网络访问管理器、ISE 终端安全评估、客户体验反馈和网络安全的配置设置。在 AnyConnect 安装和更新过程中，ASA 将部署配置文件。用户无法管理或修改配置文件。

您可以配置 ASA 或 ISE，以向所有 AnyConnect 用户全局部署配置文件，或基于用户的组策略向用户部署。通常情况下，对于安装的每个 AnyConnect 模块，用户都有一个配置文件。在某些情况下，您可能希望为用户提供多个 VPN 配置文件。在多个位置工作的某些用户可能需要多个 VPN 配置文件。

某些配置文件设置本地存储在用户计算机的用户首选项文件或全局首选项文件中。用户文件包含 AnyConnect 客户端在客户端 GUI 的“首选项”(Preferences) 选项卡中显示用户可控设置所需的信息，以及有关上一次连接的信息，例如用户、组和主机。

全局文件包含有关用户可控设置的信息，因此您可以在登录之前应用这些设置（因为此时无用户）。例如，客户端需要了解登录前是否已启用“登录前启动”(Start Before Login) 和/或“启动时自动连接”(AutoConnect On Start) 功能。

AnyConnect 配置文件编辑器，首选项（第 1 部分）

- **使用登录前启动 (Use Start Before Login)** -（仅限 Windows）启用“登录前启动”(Start Before Login) 以供客户端使用。启用“在登录前启动”(Start Before Login) 后，AnyConnect 会在 Windows 登录对话框出现之前启动。用户会在登录 Windows 之前通过 VPN 连接到企业基础设施。进行身份验证之后，将会显示登录对话框，用户可以像平常一样登录。
- **显示预连接消息 (Show Pre-connect Message)** - 支持管理员在用户首次尝试连接之前显示一条一次性消息。例如，此消息可以提醒用户将智能卡插入读卡器。此消息出现在 AnyConnect 消息目录中并已本地化。
- **客户端证书存储库 (Client Certificate Store)** - 控制 AnyConnect 使用哪个证书存储库来读取客户端证书。必须相应地配置安全网关，并命令客户端可以接受多个证书身份验证组合中的哪一个用于特定 VPN 连接。

  安全网关可接受的证书类型：两个用户证书，或者一个计算机证书和一个用户证书。

若要允许证书存储库的访问由 AnyConnect 进一步筛选，您可以从 Windows、macOS 或 Linux 下拉菜单配置证书存储库。配置文件首选项支持以下值：

- **Windows 的 ISE 安全评估代理**
- 全部 (All) - [默认]使用来自 Windows 计算机和用户证书存储库的客户端证书。
- 计算机 (Machine) - 仅使用 Windows 证书存储库中的客户端证书。
- 用户 (User) - 仅使用 Windows 证书存储库中的客户端证书。
- **macOS**
- 全部 (All) - [默认]使用所有可用密钥链和 PEM 文件存储区的客户端证书。
- 系统 (System) - 仅使用系统密钥链和系统 PEM 文件存储区的客户端证书。
- 登录 (Login) - 仅使用用户登录和动态智能卡密钥链以及用户 PEM 文件存储区的客户端证书。
- **Linux**
- 全部 (All) - [默认]使用系统和用户 PEM 文件存储区以及用户 Firefox NSS 存储区的客户端证书。
- 计算机 (Machine) - 仅使用系统 PEM 文件存储区的客户端证书。
- 用户 (User) - 仅使用用户 PEM 文件存储区以及用户 Firefox NSS 存储区的客户端证书。

- **Windows 证书存储库覆盖 (Windows Certificate Store Override)** - 允许管理员指示 AnyConnect 在 Windows 计算机（本地系统）证书存储库中利用证书，以进行客户端证书身份验证。证书存储区覆盖仅适用于 SSL，默认情况下，UI 进程启动连接。使用 IPSec/IKEv2 时，AnyConnect 配置文件中的此功能不适用。

  注释 为了使用计算机证书与 Windows 连接，您必须具有预部署的配置文件并且启用了此选项。如果在连接之前 Windows 设备上不存在此配置文件，则在计算机存储库中无法访问证书，因而连接将失败。

  - **True** - AnyConnect 将在 Windows 计算机证书存储库中搜索证书。客户端证书库 (Windows) 必须设置为全部 *(All)* 或计算机 *(Machine)*。
  - **错误 (False)** —[默认]当用户没有管理权限时，AnyConnect 不在 Windows 计算机证书存储库中搜索证书。

- **AutomaticCertSelection** - 当在安全网关上配置了多重证书身份验证时，您必须将此值设置为 **true**。

- **启动时自动连接 (Auto Connect on Start)** - 启动时，AnyConnect 自动与 AnyConnect 配置文件指定的安全网关建立 VPN 连接，或者连接到客户端连接到的最后一个网关。
- **Minimize On Connect** - 建立 VPN 连接后，AnyConnect GUI 最小化。
- **Local LAN Access** - 允许用户在与 ASA 的 VPN 会话期间完成对连接到远程计算机的本地 LAN 的访问。

注释 若启用本地 LAN 访问，则用户计算机进入企业网络可能导致来自公共网络的安全漏洞。或者，您可以配置安全设备（版本 8.4 (1) 或更高版本）来部署一个 SSL 客户端防火墙，该防火墙使用默认组策略中包含的 AnyConnect 客户端本地打印防火墙规则。要启用此防火墙规则，您还必须在此编辑器的Preferences（第 2 部分）中启用 Automatic VPN Policy、Always on 和 Allow VPN Disconnect。

- **禁用强制网络门户检测** - 当 AnyConnect 客户端收到的证书的常用名与 ASA 名称不一致时，检测强制网络门户。此行为提示用户进行身份验证。使用自签名证书的某些用户可能要启用到 HTTP 强制网络门户后台的企业资源的连接，因此应选中**禁用强制网络门户检测 (Disable Captive Portal Detection)**复选框。管理员还可以确定他们是否希望该选项为用户可配置的选项，并相应地选中该复选框。如果选择用户可配置，则该复选框将出现在 AnyConnect 安全移动客户端 UI 的“首选项”(Preferences) 选项卡上。
- **自动重连** - 连接丢失时，AnyConnect 尝试重新建立 VPN 连接（默认为启用）。如果禁用 Auto Reconnect，则无论连接出于何种原因断开连接，都不会尝试重新连接。

注释 在用户能够控制客户端行为的情形下，可以使用 Auto Reconnect。AlwaysOn 不支持此功能。

  - **自动重新连接行为**
    - DisconnectOnSuspend - AnyConnect 在系统暂停时释放分配给 VPN 会话的资源，并且在系统恢复后不尝试重新连接。
    - ReconnectAfterResume（默认值）- 连接丢失时，AnyConnect 尝试重新建立 VPN 连接。

- **自动更新 (Auto Update)** - 选中此选项时，将启用客户端的自动更新。如果选中“用户可控制”(User Controllable)，则用户可以在客户端覆盖此设置。
- **RSA 安全 ID 集成**（仅限 Windows）- 控制用户如何与 RSA 交互。默认情况下，AnyConnect 确定 RSA 交互的正确方法（自动设置：软件或硬件令牌均接受）。
- **Windows 登录强制** - 允许从远程桌面协议 (RDP) 会话建立 VPN 会话。必须在组策略中配置分割隧道。当建立 VPN 连接的用户注销时，AnyConnect 会断开 VPN 连接。如果连接由远程用户建立，则该远程用户注销时 VPN 连接会终止。

- 单一本地登录 (Single Local Logon)（默认设置）-（本地：1，远程：无限制）在整个 VPN 连接期间只允许一个本地用户登录。此外，当一个或多个远程用户登录到客户端 PC 时，本地用户可以建立 VPN 连接。此设置对通过 VPN 连接从企业网络登录的远程用户没有影响。

  注释 如果为全有或全无隧道配置了 VPN 连接，则修改 VPN 连接的客户端 PC 路由表会导致远程登录断开连接。如果 VPN 连接进行了分割隧道配置，远程登录可能会也可能不会断开连接，这取决于 VPN 连接的路由配置。

- 单一登录 (Single Logon) -（本地 + 远程：1）在整个 VPN 连接期间仅允许一个用户登录。如果通过本地或远程登录的用户不止一个，则在建立 VPN 连接时，将不允许该连接。如果 VPN 连接期间有第二个用户通过本地或远程登录，则 VPN 连接将终止。由于在 VPN 连接期间不允许进行其他登录，所以无法通过 VPN 连接进行远程登录。

  注释 不支持多个用户同时登录。

- 单一登录无远程 (Single Logon No Remote) -（本地：1，远程：0）在整个 VPN 连接期间只允许一个本地用户登录。不允许任何远程用户。如果在建立 VPN 连接后，有多个本地用户或任何远程用户登录，则将不允许此连接。如果 VPN 连接期间有第二个本地用户或任何远程用户登录，则此 VPN 连接将终止。

- **Windows VPN Establishment** - 确定当远程登录到客户端 PC 的用户建立 VPN 连接时 AnyConnect 的行为。可能的值包括：

  - Local Users Only（默认值）- 阻止远程登录用户建立 VPN 连接。此功能与 AnyConnect 早期版本中的功能相同。
  - Allow Remote Users - 允许远程用户建立 VPN 连接。但是，如果所配置的 VPN 连接路由导致远程用户断开连接，则 VPN 连接会终止，以允许远程用户重新获得对客户端 PC 的访问权限。如果远程用户想要断开其远程登录会话而不终止 VPN 连接，则必须在 VPN 建立后等待 90 秒钟。

- **Linux 登录强制** - 允许从 SSH 会话建立 VPN 会话。必须在组策略中配置分割隧道。当建立 VPN 连接的用户注销时，AnyConnect 会断开 VPN 连接。如果连接由远程用户建立，则该远程用户注销时 VPN 连接会终止。

  - 单一本地登录 (Single Local Logon)（默认设置）-（本地：1，远程：无限制）在整个 VPN 连接期间只允许一个本地用户登录。此外，当一个或多个远程用户登录到客户端 PC 时，本地用户可以建立 VPN 连接。此设置对通过 VPN 连接从企业网络登录的远程用户没有影响。

注释 如果为全有或全无隧道配置了 VPN 连接，则修改 VPN 连接的客户端PC路由表会导致远程登录断开连接。如果VPN连接进行了分割隧道配置，远程登录可能会也可能不会断开连接，这取决于 VPN 连接的路由配置。

- 单一登录 (Single Logon) -（本地 + 远程：1）在整个 VPN 连接期间仅允许一个用户登录。如果通过本地或远程登录的用户不止一个，则在建立VPN连接时，将不允许该连接。如果 VPN 连接期间有第二个用户通过本地或远程登录，则 VPN 连接将终止。由于在 VPN 连接期间不允许进行其他登录，所以无法通过 VPN 连接进行远程登录。

注释 不支持多个用户同时登录。

- 单一登录无远程 (Single Logon No Remote) -（本地：1，远程：0）在整个 VPN 连接期间只允许一个本地用户登录。不允许任何远程用户。如果在建立VPN连接后，有多个本地用户或任何远程用户登录，则将不允许此连接。如果VPN连接期间有第二个本地用户或任何远程用户登录，则此 VPN 连接将终止。

- **Linux VPN 建立** - 确定当登录到客户端 PC 的用户使用 SSH 建立 VPN 连接时 AnyConnect 的行为。可能的值包括：
  - 仅限本地用户（默认值）- 阻止远程登录用户建立 VPN 连接。
  - 允许远程用户 - 允许远程用户建立 VPN 连接。
- **Clear SmartCard PIN**
- **支持的 IP 协议** - 若同时具有 IPv4 和 IPv6 地址的客户端尝试使用 AnyConnect 连接到 ASA，AnyConnect 需要决定使用哪种 IP 协议发起连接。默认情况下，AnyConnect 先使用 IPv4 尝试连接。如果这样不成功，AnyConnect 将尝试使用 IPv6 发起连接。

  此字段配置初始 IP 协议和回退顺序。
  - IPv4 - 仅可建立到 ASA 的 IPv4 连接。
  - IPv6 - 仅可建立到 ASA 的 IPv6 连接。
  - IPv4, IPv6 - 先尝试建立到 ASA 的 IPv4 连接。如果客户端无法使用 IPv4 建立连接，则尝试建立 IPv6 连接。
  - IPv6, IPv4 - 先尝试建立到 ASA 的 IPv6 连接。如果客户端无法使用 IPv6 进行连接，则尝试进行 IPv4 连接。

注释 IP 协议的故障转移也可能发生在 VPN 会话期间。无论是在 VPN 会话之前还是在 VPN 会话期间执行，都会保持故障转移直到无法访问当前使用的安全网关 IP 地址。每当无法访问当前使用的 IP 地址时，客户端就会故障转移到与备用 IP 协议（如果可用）匹配的 IP 地址。

AnyConnect 配置文件编辑器，首选项（第 2 部分）

- **禁用自动证书选择 (Disable Automatic Certificate Selection)**（仅限 Windows）- 禁止客户端自动选择证书并提示用户选择身份验证证书。

  相关主题：配置证书选择

- **代理设置** - 在 AnyConnect 配置文件中指定一个策略来控制客户端对代理服务器的访问。当代理配置阻止用户从企业网络外部建立隧道时，使用此设置。
  - Native - 让客户端既使用以前由 AnyConnect 配置的代理设置，也使用在浏览器中配置的代理设置。在全局用户首选项中配置的代理设置优先于浏览器代理设置。
  - IgnoreProxy - 忽略用户计算机上的浏览器代理设置。
  - Override - 手动配置公共代理服务器的地址。公共代理是唯一一种支持 Linux 的代理类型。Windows 也支持公共代理。您可以将公共代理地址配置为 User Controllable。

- **允许本地代理连接** - 默认情况下，AnyConnect 让 Windows 用户通过本地 PC 上的透明或不透明代理服务建立 VPN 会话。如果要禁用对本地代理连接的支持，请取消选中此参数。例如，某些无线数据卡提供的加速软件和某些防病毒软件上的网络组件都可提供透明代理服务

- **启用最佳网关选择** (OGS)，（仅限 IPv4 客户端）- AnyConnect 根据往返时间 (RTT) 确定并选择哪个安全网关对于连接或重新连接是最佳选择，从而尽可能缩短互联网流量延迟，而且无需用户干预。OGS 不是安全功能，它不会在安全网关集群之间或集群内执行负载均衡。您控制 OGS 的激活和取消激活，并指定最终用户是否可以自己控制此功能。“自动选择”(Automatic Selection) 显示在客户端 GUI 的“连接”(Connection) 选项卡中的“连接到”(Connect To) 下拉列表中。
  - **暂停时间阈值 (Suspension Time Threshold)**（小时）- 输入在调用新网关选择计算之前 VPN 必须已暂停的最短时间（以小时为单位）。通过优化此值以及下一个可配置的参数“性能改进阈值”(Performance Improvement Threshold)，您可以在选择最佳网关和减少强制重新输入凭证次数之间找到适当的平衡。
  - **性能改进阈值** (%) - 在系统恢复后触发客户端重新连接到另一个安全网关的性能改进百分比。为特定网络调整这些值，可在选择最佳网关与减少次数之间找到合适的平衡，从而强制重新输入凭证。默认值为 20%。

  当 OGS 启用时，建议您也将此功能设置为用户可控制。

OGS 存在以下限制：

- 不能在设置为 Always On 的情况下运行
- 它不支持自动代理检测
- 它不支持代理自动配置 (PAC) 文件
- 如果使用 AAA，则在过渡到另外一个安全网关时，用户可能必须重新输入凭证。使用证书可消除此问题。

- **自动 VPN 策略**（仅限 Windows 和 Mac）- 启用“受信任网络检测”可使 AnyConnect 根据“受信任网络策略”和“不受信任网络策略”自动管理何时启动或停止 VPN 连接。如果禁用，则 VPN 连接只能手动启动和停止。设置 Automatic VPN Policy 不会阻止用户手动控制 VPN 连接。
  - **Trusted Network Policy** - 当用户处于企业网络（受信任网络）中时，AnyConnect 对 VPN 连接自动采取的操作。
    - Disconnect（默认值）- 检测到受信任网络时断开 VPN 连接。
    - Connect - 检测到受信任网络时发起 VPN 连接。
    - 不执行任何操作 - 在不受信任的网络中不执行任何操作。将 Trusted Network Policy 和 Untrusted Network Policy 都设置为 Do Nothing 会禁用 Trusted Network Detection。
    - Pause - 如果用户在受信任网络外建立 VPN 会话之后进入被配置为受信任的网络，则 AnyConnect 会暂停此 VPN 会话而不是将其断开连接。当用户再次离开受信任网络时，AnyConnect 会恢复该会话。此功能是为了给用户提供方便，因为有了它，在用户离开受信任网络后不需要建立新的 VPN 会话。
  - **不受信任网络策略** - 当用户处于企业网络外（不受信任的网络）时，AnyConnect 启动 VPN 连接。此功能可以在用户处于受信任网络外时发起 VPN 连接，从而鼓励提高安全意识。
    - Connect（默认值）- 在检测到不受信任网络时发起 VPN 连接。
    - Do Nothing - 在受信任网络中不执行任何操作。此选项禁用永远在线 VPN。将 Trusted Network Policy 和 Untrusted Network Policy 都设置为 Do Nothing 会禁用 Trusted Network Detection。
  - **Trusted DNS Domains** - 客户端处于受信任网络中时，网络接口可能具有的 DNS 后缀（逗号分隔的字符串）。例如：*.cisco.com。DNS 后缀支持通配符 (*)。

注释 如果您使用的是 NVM，则不支持受信任的 DNS 域和服务器，因为 NVM 模块使用管理员定义的受信任服务器和证书散列来确定用户位于受信任还是不受信任的网络上。

- **受信任 DNS 服务器** - 客户端处于受信任网络中时，网络接口可能具有的 DNS 服务器地址（逗号分隔的字符串）。例如：192.168.1.2, 2001:DB8::1。IPv4 或 IPv6 DNS 服务器地址支持通配符 (*)。

- **Trusted Servers @ https://<server>[:<port>]** - 要添加为受信任的主机 URL。在单击**添加 (Add)** 后，将会添加 URL 并预填充证书哈希值。如果未找到哈希值，系统将显示一条错误消息，提示用户手动输入证书哈希值并单击**设置 (Set)**。

  可信 URL 要求必须存在一个安全 Web 服务器，且可通过可信任证书对其进行访问。安全 TND 尝试连接到列表中第一个已配置的服务器。如果无法联系到服务器，安全 TND 将尝试联系已配置列表中的下一台服务器。如果可以联系到服务器，但证书的哈希值不匹配，则网络将被标识为“不可信”。系统不会评估其他服务器。如果哈希值受信任，则满足“受信任”条件。

  注释 只有当一个或以上的受信任的 DNS 域或 DNS 服务器被定义时，您才可以配置该参数。如果受信任的 DNS 域或 DNS 服务器未被定义，则该字段将被禁用。

- **始终在线 (Always On)** - 确定当用户登录到运行受支持的 Windows 或 macOS 操作系统的计算机时，AnyConnect 是否自动连接到 VPN。您可以实施企业策略，以便在计算机不在受信任网络中时阻止计算机访问互联网资源，从而保护它免遭安全威胁。根据分配策略所用的匹配条件，您可以指定异常情况，从而在组策略和动态访问策略中设置永远在线 VPN 参数来覆盖此设置。如果 AnyConnect 策略启用永远在线，而动态访问策略或组策略禁用它，只要其条件匹配关于建立每个新会话的动态访问策略或组策略，客户端就为当前和将来的 VPN 会话保留此禁用设置。在启用后，您就可以配置其他参数。

  注释 AlwaysOn 用于连接建立和冗余运行而无需用户干预的情形；因此，在使用此功能时，您不需要配置或启用 Preferences 第 1 部分中的 Auto Reconnect。

  相关主题：需要使用 永远在线 的 VPN 连接

  - **Allow VPN Disconnect** - 确定 AnyConnect 是否为永远在线 VPN 会话显示 Disconnect 按钮。由于当前 VPN 会话存在性能问题或 VPN 会话中断后重新连接出现问题，永远在线 VPN 会话的用户可能想要单击“断开连接”(Disconnect) 以选择其他安全网关。

    Disconnect 会锁定所有接口，以防止数据泄漏并防止计算机在建立 VPN 会话外还以其他方式访问互联网。出于上述原因，禁用 Disconnect 按钮有时可能会阻碍或防止 VPN 接入。

  - **允许在 VPN 断开连接时访问以下主机 (Allow Access to the Following Hosts With VPN Disconnected)** - 当 VPN 在永远在线期间断开连接时，允许终端访问已配置的主机。值是主机的逗号分隔列表，可以是指定 IP 地址、IP 地址范围（CIDR 格式）或 FQDN。最多允许 500 个主机，并且不支持通配符。

警告：对指定 FQDN 的访问取决于在不受信任网络中执行的名称解析。

- **Connect Failure Policy** - 确定在 AnyConnect 无法建立 VPN 会话（例如，无法访问 ASA）时计算机是否可访问互联网。此参数只在启用了永远在线和 Allow VPN Disconnect 时才适用。如果选择永远在线，则 fail-open 策略允许网络连接，fail-close 策略禁用网络连接。
  - Closed - 当无法访问 VPN 时限制网络访问。此设置的目的是，当负责保护终端的专用网络中的资源不可用时，帮助保护企业资产免遭网络威胁。
  - Open - 当无法访问 VPN 时允许网络访问。

注意 如果 AnyConnect 未能建立 VPN 会话，连接故障关闭策略会阻止网络访问。它主要用在网络访问的安全持久性比始终可用性更重要的企业中，以特别保证企业的安全。除本地资源（例如，分隔隧道允许和 ACL 限制的打印机和系留设备等）外，它会阻止所有网络访问。如果用户在安全网关不可用时需要 VPN 以外的互联网接入，它可能停止运行。AnyConnect 检测大多数强制网络门户。如果它不能检测到强制网络门户，连接故障关闭策略会阻止所有网络连接。

如果您部署关闭连接策略，我们强烈建议您采用分阶段方法。例如，首先利用连接失败打开策略部署永远在线 VPN，并调查用户 AnyConnect 无法无缝连接的频率。然后，在早期采用者用户中部署连接失败关闭策略的一个小型试点部署，并征求他们的反馈。逐步扩展试点计划，同时继续征求反馈，再考虑全面部署。部署连接失败关闭策略时，请确保向 VPN 用户告知网络访问限制以及连接失败关闭策略的优点。

相关主题：关于强制网络门户

如果 Connect Failure Policy 为 Closed，则您可以配置以下设置：

- **Allow Captive Portal Remediation** - 当客户端检测到强制网络门户（热点）时，让 AnyConnect 解除关闭连接失败策略所施加的网络访问限制。酒店和机场通常使用强制网络门户，它们要求用户打开浏览器并满足允许互联网访问所需的条件。默认情况下，此参数处于未选中状态可提供最高安全性。但是，如果您想要客户端连接到 VPN 而强制网络门户却阻止它这样做，则您必须启用此参数。
- **Remediation Timeout** - AnyConnect 解除网络访问限制的分钟数。此参数只在“允许强制网络门户补救”(Allow Captive Portal Remediation) 参数被选中且客户端检测到强制网络门户时适用。指定满足一般强制网络门户要求所需的足够时间（例如，5 分钟）。

- **Apply Last VPN Local Resource Rules** - 如果 VPN 无法访问，则客户端应用其从 ASA 收到的最后一个客户端防火墙，此 ASA 可能包含允许访问本地 LAN 资源的 ACL。

相关主题：配置连接失败策略

- **强制网络门户补救浏览器故障转移 (Captive Portal Remediation Browser Failover)** - 允许最终用户使用外部浏览器（在关闭 AnyConnect 浏览器后）进行强制网络门户补救。

  请参阅使用强制网络门户热点检测和补救，第 119 页获得更多信息。

- **Allow Manual Host Input** - 支持用户输入与 AnyConnect UI 的下拉框中所列内容不同的 VPN 地址。如果取消选中此复选框，VPN 连接将仅限于下拉框中的选项，并且用户只能输入新的 VPN 地址。

- **PPP Exclusion** - 对于通过 PPP 连接的 VPN 隧道，指定是否以及如何确定排除路由。客户端可以将去往此安全网关的流量从去往安全网关外目标的隧道流量中排除。排除路由在 AnyConnect GUI 的 Route Details 中显示为非安全路由。如果将此功能设置为用户可控制，则用户能够读取和更改 PPP 排除设置。

  - Automatic - 启用 PPP 排除。AnyConnect 自动确定 PPP 服务器的 IP 地址。
  - 覆盖 (Override) - 使用 *PPP Exclusion Server IP*（*PPP* 排除服务器 *IP*）字段中指定的预定义服务器 IP 地址来启用 PPP 排除。*PPP* 排除服务器 *IP (PPP Exclusion Server IP)* 字段仅适用于此覆盖方法，并且仅在“自动”(Automatic) 选项无法检测 PPP 服务器的 IP 地址时使用。

    为“PPP 排除服务器 IP”(PPP Exclusion Server IP) 选中**用户可控制 (User Controllable)** 字段可允许最终用户通过 preferences.xml 文件手动更新 IP 地址。请参阅指示用户覆盖 PPP 排除，第 122 页一节。
  - Disabled - 不应用 PPP 排除。

- **启用脚本 (Enable Scripting)** - 如果安全设备闪存上存在 OnConnect 和 OnDisconnect 脚本，则启动它们。

  - **Terminate Script On Next Event** - 发生向另一个可编写脚本事件的过渡时终止正在运行的脚本进程。例如，如果 VPN 会话结束，则 AnyConnect 终止正在运行的 OnConnect 脚本。如果客户端启动新的 VPN 会话，则终止正在运行的 OnDisconnect 脚本。在 Microsoft Windows 上，客户端还会终止 OnConnect 或 OnDisconnect 脚本启动的任何脚本以及它们的所有脚本子代。在 macOS 和 Linux 上，客户端只会终止 OnConnect 或 OnDisconnect 脚本，它不会终止子脚本。
  - **Enable Post SBL On Connect Script** - 启动 OnConnect 脚本（如果存在），然后 SBL 建立 VPN 会话。（仅当 VPN 终端运行 Microsoft Windows 时才受支持。）

- **注销时保留 VPN (Retain VPN On Logoff)** - 确定是否在用户注销 Windows 或 Mac 操作系统时保留 VPN 会话。

- **User Enforcement** - 指定当其他用户登录时是否结束 VPN 会话。此参数仅在“注销时保留 VPN”(Retain VPN On Logoff) 被选中且原始用户在 VPN 会话进行中注销 Windows 或 macOS 时适用。

- **Authentication Timeout Values** - 默认情况下，AnyConnect 在终止连接尝试前，要等待长达 30 秒才能从安全网关获得身份验证。然后，AnyConnect 显示一条消息，指示身份验证已超时。输入介于 10 - 120 之间的秒数。

AnyConnect 配置文件编辑器，备用服务器

您可以配置一个备用服务器列表，以便客户端在用户选择的服务器发生故障时使用。如果用户选择的服务器发生故障，客户端会尝试连接到在列表顶端的最佳服务器备用。如果该尝试失败了，客户端会按其选择结果依次尝试最佳网关选择列表中剩余的每个服务器。

注释 仅当未在 AnyConnect 配置文件编辑器，添加/编辑服务器列表，第 90 页中定义备用服务器时，才会尝试使用您在此处配置的任何备用服务器。在 Server List 中配置的服务器优先，而此处列出的备用服务器将被覆盖。

主机地址 (Host Address) - 指定一个 IP 地址或完全限定域名 (FQDN) 以包含在备用服务器列表中。

- **添加 (Add)** - 将主机地址添加到备用服务器列表。
- **上移 (Move Up)** - 将选定的备用服务器在列表中向上移动。如果用户选择的服务器发生故障，则客户端首先尝试连接到此列表顶端的备用服务器，必要时再沿着列表从上到下逐个尝试。
- **下移 (Move Down)** - 将选定的备用服务器在列表中向下移动。
- **删除 (Delete)** - 从服务器列表中删除备用服务器。

AnyConnect 配置文件编辑器，证书匹配

启用可用于优化此窗格中自动客户端证书选择的各属性的定义。

如果未指定证书匹配条件，则 AnyConnect 应用以下证书匹配规则：

- Key Usage：Digital_Signature
- Extended Key Usage：Client Auth

如果配置文件中指定了任何条件匹配规范，则不应用这些匹配规则，除非配置文件中具体列出了这些规则。

- **密钥使用 (Key Usage)** - 在选择可接受的客户端证书时，使用以下证书密钥属性：
  - Decipher_Only - 解密数据，且未设置其他位（Key_Agreement 除外）。
  - Encipher_Only - 加密数据，且未设置其他位（Key_Agreement 除外）。

- CRL_Sign - 验证 CRL 上的 CA 签名。
- Key_Cert_Sign - 验证证书上的 CA 签名。
- Key_Agreement - 密钥协议。
- Data_Encipherment - 加密除 Key_Encipherment 以外的数据。
- Key_Encipherment - 加密密钥。
- Non_Repudiation - 验证数字签名保护，以免错误拒绝某些操作（Key_Cert_sign 或 CRL_Sign 除外）。
- Digital_Signature - 验证数字签名（Non_Repudiation、Key_Cert_Sign 或 CRL_Sign 除外）。

- **Extended Key Usage** - 使用以下 Extended Key Usage 设置。OID 括在括号内：
  - ServerAuth (1.3.6.1.5.5.7.3.1)
  - ClientAuth (1.3.6.1.5.5.7.3.2)
  - CodeSign (1.3.6.1.5.5.7.3.3)
  - EmailProtect (1.3.6.1.5.5.7.3.4)
  - IPSecEndSystem (1.3.6.1.5.5.7.3.5)
  - IPSecTunnel (1.3.6.1.5.5.7.3.6)
  - IPSecUser (1.3.6.1.5.5.7.3.7)
  - TimeStamp (1.3.6.1.5.5.7.3.8)
  - OCSPSign (1.3.6.1.5.5.7.3.9)
  - DVCS (1.3.6.1.5.5.7.3.10)
  - IKE Intermediate

- **Custom Extended Match Key**（最多 10 个）- 指定定制扩展匹配密钥（如果有，最多 10 个）。证书必须与您输入的所有指定密钥匹配。以 OID 格式（例如 1.3.6.1.5.5.7.3.11）输入密钥。

注释 如果创建的一个定制扩展匹配密钥的 OID 大小超过 30 个字符，则您单击“确定 (OK)”按钮时，该密钥不会被接受。OID 的最大字符数限制是 30。

- **只与支持密钥用法扩展 (EKU) 的证书匹配** - 先前的做法是：如果设置了证书可分辨名称 (DN) 匹配规则，客户端会与带特定 EKU OID 和所有不带 EKU 的证书匹配。为了在保持一致性的同时提升清晰度，您可以禁止与不带 EKU 证书进行匹配。默认设置为保留客户所期待的这一传统行为。您必须通过单击复选框来启用新行为以及禁止该匹配。

- **可分辨名称 (Distinguished Name)**（最多 10 个）- 指定在选择可接受的客户端证书时用于完全匹配条件的可分辨名称 (DN)。
  - **Name** - 用于匹配的可分辨名称 (DN)：
    - CN - 主题通用名
    - C - 主题国家/地区
    - DC - 域组件
    - DNQ - 主题 DN 限定符
    - EA - 主题邮件地址
    - GENQ - 主题代际限定符
    - GN - 主题给定名称
    - I - 主题首字母缩写
    - L - 主题城市
    - N - 主题未定义的名称
    - O - 主题公司
    - OU - 主题部门
    - SN - 主题姓氏
    - SP - 主题省/自治区
    - ST - 主题州
    - T - 主题称谓
    - ISSUER-CN - 颁发者通用名
    - ISSUER-DC - 颁发者组件
    - ISSUER-SN - 颁发者姓氏
    - ISSUER-GN - 颁发者给定名称
    - ISSUER-N - 颁发者未定义的名称
    - ISSUER-I - 颁发者首字母缩写
    - ISSUER-GENQ - 颁发者代际限定符
    - ISSUER-DNQ - 颁发者 DN 限定符
    - ISSUER-C - 颁发者国家/地区
    - ISSUER-L - 颁发者城市
    - ISSUER-SP - 颁发者所在省/自治区

- ISSUER-ST - 颁发者所在州
- ISSUER-O - 颁发者所在公司
- ISSUER-OU - 颁发者所在部门
- ISSUER-T - 颁发者称谓
- ISSUER-EA - 颁发者邮件地址

- **Pattern** - 指定要匹配的字符串。要匹配的型号应仅包括要匹配的字符串部分。不需要包括型号匹配或正则表达式语法。如果输入了语法，此语法将被视为待搜索字符串的一部分。

  例如，如果示例字符串是 abc.cisco.com，且为了与 cisco.com 匹配，则输入的型号应该是 cisco.com。

- **Operator** - 为此 DN 执行匹配时使用的运算符。
  - Equal - 与 == 等效
  - Not Equal - 与 != 等效
- **Wildcard** - 启用后将包含通配符型号匹配。在通配符启用的情况下，该型号可以位于字符串的任何位置。
- **大小写匹配 (Match Case)** - 选中可启用区分大小写的型号匹配。

相关主题

配置证书匹配，第 154 页

AnyConnect 配置文件编辑器，证书注册

证书注册使 AnyConnect 能够使用简单证书注册协议 (SCEP) 调配和续订用于客户端身份验证的证书。

- **Certificate Expiration Threshold** - 在证书过期日前，AnyConnect 提醒用户其证书即将过期的天数（RADIUS 密码管理不支持该功能）。默认值为零（不显示警告）。值范围为 0 到 180 天。
- **客户端证书导入存储库 (Client Certificate Import Store)** - 选择注册证书保存至的证书存储库。
  - **Windows 的 ISE 安全评估代理**
  - 全部 (All) — [默认]将注册证书导入 Windows 计算机和用户证书库。
  - 计算机 (Machine) — 仅将注册证书导入 Windows 计算机证书存储库。
  - 用户 (User) — 仅将注册证书导入 Windows 用户证书存储库。
  - **Linux**
  - 全部 (All) — [默认]将注册证书导入用户 PEM 文件和用户 Firefox NSS 证书存储库。
  - UserFirefoxNSS — 仅将注册证书导入用户 Firefox NSS 证书存储库。

- UserPEMFile — 仅将注册证书导入用户 PEM 文件证书存储库。

- **macOS**
- 注册证书只能被导入到用户登录密钥链中。
- **移动平台**
- 注册证书只能被导入到应用程序沙盒。

- **Certificate Contents** - 指定要包含在 SCEP 注册请求中的证书内容：
  - 名称 (CN) - 证书中的通用名。
  - 部门 (OU) - 证书中指定的部门名称。
  - 公司 (O) - 证书中指定的公司名称。
  - 州 (ST) - 证书中指定的州标识符。
  - 州 (SP) - 另一个州标识符。
  - 国家/地区 (C) - 证书中指定的国家/地区标识符。
  - 邮件 (EA) - 邮件地址。以下示例中，邮件地址 (EA) 为 %USER%@cisco.com。%USER% 对应用户的 ASA 用户名登录凭证。
  - 域 (DC) - 域组件。在以下示例中，域 (DC) 设置为 cisco.com。
  - 姓氏 (SN) - 家族名或姓。
  - 给定名称 (GN) - 通常为名。
  - UnstructName (N) - 未定义的名称。
  - 首字母缩写 (I) - 用户的首字母缩写。
  - 限定符 (GEN) - 用户的代限定符。例如，“Jr.”或“III.”
  - 限定符 (DN) - 整个 DN 的限定符。
  - 城市 (L) - 城市标识符。
  - 称谓 (T) - 人员的称谓。例如，女士、夫人、先生
  - CA 域 - 用于 SCEP 注册，一般为 CA 域。
  - 密钥大小 - 为待注册证书所生成的 RSA 密钥的大小。

- **Display Get Certificate Button** - 启用 AnyConnect GUI 可在下列条件下显示 Get Certificate 按钮：
  - 证书设置为在证书过期阈值定义的时间段后过期（RADIUS 不支持）。
  - 证书已过期。
  - 证书不存在。

- 证书无法匹配。

相关主题

配置证书注册，第 146 页

AnyConnect 配置文件编辑器，证书锁定

必备条件

开始证书锁定之前，请参阅关于证书锁定，第 163 页了解最佳实践。

使用 VPN 配置文件编辑器启用首选项，并配置全局证书锁定和按主机证书锁定。如果在“全局锁定”(Global Pins) 部分中启用了首选项，则只能在服务器列表部分中按主机锁定证书。启用该首选项后，可以配置一个全局锁定列表，供客户端进行证书锁定验证使用。在服务器列表部分中添加按主机锁定与添加全局锁定类似。您可以锁定证书链中的任何证书，这些证书会被导入配置文件编辑器以计算锁定所需的信息。

添加锁定 (Add Pin) - 启动证书锁定向导，该向导会指导您将证书导入配置文件编辑器并锁定它们。

该窗口的证书详细信息部分允许您直观地验证“主题 (Subject)”和“颁发者 (Issuer)”列。

证书锁定向导

您可以将服务器证书链的任何证书导入到配置文件编辑器中，以指定锁定所需的信息。配置文件编辑器支持三个证书导入选项：

- 浏览本地文件 (Browse Local Files) - 选择本地存在于计算机上的证书。
- 从 URL 下载文件 (Download file from a URL) - 从任何文件托管服务器下载证书。
- 粘贴 PEM 格式的信息 (Paste information in PEM format) - 以 PEM 格式插入信息，包括证书开始报头和结束报头。

注释 您仅可导入 DER、PEM 和 PKCS7 数据格式的证书。

AnyConnect 配置文件编辑器，移动策略

AnyConnect 3.0 版及更高版本不支持 Windows Mobile 设备。请参阅 *Cisco AnyConnect Secure Mobility Client* 管理员指南，版本 *2.5*，了解 Windows Mobile 设备的相关信息。

AnyConnect 配置文件编辑器，服务器列表

您可以配置在客户端GUI中显示的服务器列表。用户可以在该列表中选择服务器以建立VPN连接。

服务器列表表列：

- 主机名 - 用于指代主机、IP 地址或完全限定域名 (FQDN) 的别名。
- 主机地址 - 服务器的 IP 地址或 FQDN。
- 用户组 - 用于与主机地址一同组成基于组的 URL。
- 自动 SCEP 主机 - 为调配和续订进行客户端身份验证的证书而指定的简单证书注册协议。
- CA URL - 此服务器用于连接到证书颁发机构 (CA) 的 URL。
- 证书锁定 - 在锁定验证期间，由客户端使用的按主机锁定。请参阅 AnyConnect 配置文件编辑器，证书锁定，第 89 页。

注释 客户端在锁定验证期间使用全局锁定和对应的按主机锁定。按主机锁定的配置方式类似于使用证书锁定向导配置全局锁定的方式。

Add/Edit - 启动 Server List Entry 对话框，您可在此指定上述服务器参数。

Delete - 从服务器列表中删除服务器。

Details - 显示有关备用服务器或服务器 CA URL 的更多详细信息。

相关主题

配置 VPN 连接服务器，第 107 页

AnyConnect 配置文件编辑器，添加/编辑服务器列表

- **Host Display Name** - 输入用于指代主机的别名、IP 地址或完全限定域名 (FQDN)。
- **FQDN or IP Address** - 指定服务器的 IP 地址或 FQDN。
  - 如果在 Host Address 字段中指定了 IP 地址或 FQDN，则 Host Name 字段中的条目会变成 AnyConnect 客户端弹出式托盘的连接下拉列表中的服务器标签。
  - 如果仅在 Hostname 字段中指定了 FQDN，而未在 Host Address 字段中指定 IP 地址，则 Hostname 字段中的 FQDN 将由 DNS 服务器进行解析。
  - 如果输入 IP 地址，请使用安全网关的公共 IPv4 地址或全局 IPv6 地址。不支持使用链路本地安全网关地址。
- **User Group** - 指定一个用户组。

  用户组用于与主机地址一起形成一个基于组的URL。如果指定主要协议为IPsec，则用户组必须是连接配置文件（隧道组）的确切名称。对于 SSL，用户组是连接配置文件的 group-url。

注释 在 IKEv2/IPsec 连接中，当无法访问主服务器时，为主服务器输入的 **User Group**（用户组）信息会转发到备份服务器。要使 SSL 具有相同的行为，还必须将用户组信息作为 URL（例如，https://example.com/usergroup）而不只是 FQDN 提供给备份服务器。

- **附加的仅限移动的设 (Additional mobile-only settings)** - 选择此项可配置 Apple iOS 和 Android 移动设备。
- **Backup Server List**

  我们建议您配置一个备用服务器列表，以便客户端在用户选择的服务器发生故障时使用。如果服务器发生故障，则客户端首先尝试连接到此列表顶端的服务器，必要时再沿着列表从上到下逐个尝试。

  注释 相反，在 AnyConnect 配置文件编辑器，备用服务器，第 84 页中配置的备用服务器是所有连接条目的全局条目。在配置文件编辑器的备份服务器中输入的任何条目都会被这里的备份服务器列表中的单个服务器列表条目所覆盖。此设置优先，并且是推荐做法。

  - **Host Address** - 指定一个 IP 地址或 FQDN 以包含在备用服务器列表中。如果客户端无法连接到主机，则它将尝试连接到备用服务器。
  - **Add** - 将主机地址添加到备用服务器列表。
  - **Move Up** - 将选定的备用服务器在列表中向上移动。如果用户选择的服务器发生故障，则客户端首先尝试连接到此列表顶端的备用服务器，必要时再沿着列表从上到下逐个尝试。
  - **Move Down** - 将选定的备用服务器在列表中向下移动。
  - **Delete** - 从服务器列表中删除备用服务器。

- **Load Balancing Server List**

  如果此服务器列表条目的主机是安全设备的负载均衡集群，且启用了永远在线功能，则在此列表中指定集群的备用设备。否则，永远在线会阻止对负载均衡集群中备用设备的访问。

  - **Host Address** - 指定负载均衡集群中备用设备的 IP 地址或 FQDN。
  - **Add** - 将地址添加到负载均衡备用服务器列表中。
  - **Delete** - 从列表中删除负载均衡备用服务器。

- **Primary Protocol** - 指定连接到此服务器所用的协议，即 SSL 或 IPsec（与 IKEv2 结合使用）。默认协议是 SSL。

- **仅限标准身份验证（IOS 网关）(Standard Authentication Only [IOS Gateways])** - 当选择 IPsec 作为协议时，您可以选择此选项，将连接的身份验证方法限制为 IOS 服务器。

  注释 如果此服务器是 ASA，则将身份验证方法从专有的 AnyConnect EAP 更改为基于标准的方法会禁用 ASA 的以下功能：配置会话超时、空闲超时、断开连接超时、分割隧道、拆分 DNS、MSIE 代理配置及其他功能。

- **IKE 协商期间的身份验证方法 (Auth Method During IKE Negotiation)** - 选择一种基于标准的身份验证方法。
  - **IKE 身份 (IKE Identity)** - 如果选择基于标准的 EAP 身份验证方法，您可以在此字段中输入一个组或域作为客户端标识。客户端将字符串以 ID_GROUP 型 IDi 负载的形式发送。默认情况下，此字符串是 *$AnyConnectClient$*。

- **CA URL** - 指定 SCEP CA 服务器的 URL。输入 FQDN 或 IP 地址。例如，http://ca01.cisco.com。
- **证书锁定 (Certificate Pins)** - 锁定验证期间由客户端使用的按主机锁定。请参阅AnyConnect 配置文件编辑器，证书锁定，第 89 页。
- **Prompt For Challenge PW** - 启用此项可让用户手动发出证书请求。当用户单击“获取证书”(Get Certificate) 时，客户端将提示用户输入用户名和一次性密码。
- **CA Thumbprint** - CA 的证书拇指指纹。使用 SHA1 或 MD5 哈希值。

  注释 CA 服务器管理员可以提供 CA URL 和拇指指纹。拇指指纹应直接从服务器获取，而不是从它发布的证书的 fingerprint 或 thumbprint 属性字段中获取。

相关主题

配置 VPN 连接服务器，第 107 页

AnyConnect 配置文件编辑器，移动设置

Apple iOS/Android 设置

- **证书身份验证** - 与连接条目相关的证书身份验证策略属性指定如何处理此连接的证书。有效值为：
  - **自动 (Automatic)** - AnyConnect 自动选择连接时进行身份验证所使用的客户端证书。在这种情况下，AnyConnect 将查看所有已安装的证书、忽略那些过期证书、应用 VPN 客户端配置文件中定义的证书匹配条件，然后使用与条件匹配的证书进行身份验证。每次设备用户尝试建立 VPN 连接时都会出现这种情况。

- **Manual** - AnyConnect 将在下载配置文件并执行以下任一操作时，从 Android 设备上的 AnyConnect 证书存储区中搜索证书：
  - 如果 AnyConnect 基于 VPN 客户端配置文件中定义的证书匹配条件找到一个证书，则它将该证书分配给连接条目并在建立连接时使用该证书。
  - 如果找不到匹配的证书，证书身份验证策略将设置为“自动”。
  - 如果分配的证书因任何原因从 AnyConnect 证书存储区删除，则 AnyConnect 将证书身份验证策略重置为 Automatic。
- **Disabled** - 客户端证书不用于身份验证。

- **Make this Server List Entry active when profile is imported** - 当 VPN 配置文件下载到设备时，将服务器列表条目定义为默认连接。只有一个服务器列表条目可以具有此名称。默认值为禁用。

仅适用于 Apple iOS 的设置

- **Reconnect when roaming between 3G/Wifi networks** - 该设置启用时（默认值），AnyConnect 在丢失连接、设备唤醒或连接类型发生更改（例如 EDGE(2G)、1xRTT(2G)、3G 或 Wi-Fi）后不限制用于尝试重新连接的时间。此功能提供了实现跨网络的持续安全连接的无缝移动性。此功能对于需要与企业连接的应用非常有用，但也会消耗更多的电池电量。

  如果网络漫游被禁用，且 AnyConnect 丢失连接，它在必要时尝试重新建立连接的时间最长可达 20 秒。如果无法建立连接，设备用户或应用必须启动一个新 VPN 连接（如果需要）。

  注释 网络漫游不影响数据漫游或使用多个移动服务提供商。

- **Connect on Demand**（需要证书颁发机构）- 此字段可让您配置由 Apple iOS 提供的按需连接功能。您可以创建规则列表，每当其他应用启动使用域名系统 (DNS) 解析的网络连接时都进行检查。

  按需连接仅可在 Certificate Authentication 字段设置为 Manual 或 Automatic 时使用。如果“证书身份验证”字段设置为“已禁用”，此复选框将变暗。在该复选框变暗时，仍可配置和保存由“匹配域或主机”以及“按需操作”字段定义的按需连接规则。

- 匹配域或主机 - 输入您希望为其创建按需连接规则的主机 (host.example.com)、域名 (.example.com) 或部分域 (.internal.example.com)。请勿在此字段中输入 IP 地址 (10.125.84.1)。
- 按需操作指定设备用户尝试连接上一步中定义的域或主机时执行的下列操作之一：
  - 从不连接 - iOS 在匹配此列表中的规则时从不启动 VPN 连接。此列表中的规则优先于所有其他列表。

注释 当 Connect on Demand 启用时，应用会将服务器地址自动添加到此列表中。这将防止您在尝试使用网络浏览器访问服务器的无客户端门户时自动建立 VPN 连接。如果您不希望发生此行为，请删除此规则。

- **按需连接** - iOS 仅在系统因无法使用 DNS 解析地址而匹配此列表中的规则时启动 VPN 连接。
- **Always Connect** - 始终连接行为与版本有关：
  - 在 Apple iOS 6 上，iOS 在匹配此列表中的规则时始终启动 VPN 连接。
  - iOS 7.x 上不支持 Always Connect，当此列表中的规则匹配时，其行为与 Connect If Needed 规则相同。
  - 更高版本中不使用 Always Connect，配置的规则将跳转到 Connect if Needed 列表，并按照该规则操作。
- **添加或删除** - 将“匹配域或主机”和“按需操作”字段中指定的规则添加到规则表中，或从规则表中删除所选的规则。

NVM 配置文件编辑器

在配置文件编辑器中，配置收集服务器的 IP 地址或 FQDN。您还可以自定义数据收集策略，用于选择要发送哪些类型数据，以及确定数据是否匿名。

网络可视性模块可以使用包含 IPv4 地址的单个堆栈 IPv4、包含 IPv6 地址的单个堆栈 IPv6 或双堆栈 IPv4/IPv6，建立与操作系统首选的 IP地址的连接。

移动网络可视性模块仅可以使用 IPv4 建立连接。不支持 IPv6 连接。

注释 当网络可视性模块在受信任网络中时，该模块发送流量信息。默认情况下，不收集任何数据。仅在配置文件中进行了相应配置时才会收集数据，且连接终端后，会继续收集数据。如果在一个不可信网络上进行收集，则会缓存数据，并在终端处于受信任的网络中时发送数据。如果您将收集数据发送到 Stealthwatch 7.3.1 及更低版本（或 Splunk 及类似 SIEM 工具之外的工具），则缓存数据会在受信任网络上发送一次，但不会进行处理。对于 Stealthwatch 应用程序，请参阅 Stealthwatch 企业终端许可证和 NVM 配置指南。

如果已在 NVM 配置文件中配置了 TND，则受信任的网络检测由 NVM 完成，并且不依赖于 VPN 来确定终端是否位于受信任的网络中。此外，如果 VPN 为已连接状态，则会将终端视作处于受信任网络中，并会发送流信息。NVM 特定的系统日志会显示 TND 使用情况。

直接在 NVM 配置文件中配置 TND 时，管理员定义的受信任服务器和证书散列将确定用户位于受信任还是不受信任的网络上。管理员为核心 VPN 配置文件配置 TND 会在核心 VPN 配置文件中另外配置受信任 DNS 域和受信任 DNS 服务器：AnyConnect 配置文件编辑器，首选项（第 2 部分），第 79 页。

- **桌面 (Desktop)** 或**移动 (Mobile)** - 确定是在桌面还是移动设备上设置 NVM。**桌面 (Desktop)** 是默认值。 未来将支持移动设备。
- **收集器配置**
  - **IP 地址/FQDN (IP Address/FQDN)** - 指定收集器的 IPv4 或 IPv6 IP 地址/FQDN。
  - **端口 (Port)** - 指定收集器正在侦听哪个端口号。
  - **安全 (Secure)** - 确定是否希望 NVM 通过 DTLS 安全地将数据发送到收集器。选中此复选框后，NVM 将使用 DTLS 进行传输。DTLS 连接要求终端信任 DTLS 服务器（收集器）证书。系统将以静默方式拒绝任何不受信任的证书。

    DTLS 支持需要收集器作为 CESA Splunk 应用 v3.1.0 的一部分，DTLS 1.2 是支持的最低版本。
- **缓存配置**
  - **最大大小 (Max Size)** - 指定该数据库可以达到的最大大小。以前对缓存大小有预设的限制，但您现在可在配置文件中配置它。缓存中的数据以加密格式存储，因此只有拥有根权限的进程可以解密数据。

    一旦达到大小限制，将从空间中丢弃最旧数据，将空间留给新数据。
  - **最大持续时间 (Max Duration)** - 指定您希望将数据存储多少天。如果您还设置了最大大小，则首先达到的限制优先。

    一旦达到天数限制，将从空间中丢弃日期最早的数据，将空间留给日期最近的数据。如果仅配置了“最大持续时间 (Max Duration)”，则没有大小上限；如果二者都被禁用，则大小上限为 50 MB。
- **定期模板** - 指定从终端发出模板的时间间隔。默认值为 1440 分钟

- **定期流量报告**（可选，仅应用于桌面）- 单击以启用定期流量报告。默认情况下，NVM 发送连接结束时的流量相关信息（当禁用此选项时）。如果需要定期的流量相关信息（甚至在这些流量被关闭之前），请在此处设置间隔（以秒为单位）。值为 0 表示在每个流量开始和结束时发送流量信息。如果值为 *n*，则将在每个流量开始时、每隔 *n* 秒时和结束时发送流量信息。使用此设置跟踪长期运行的连接（甚至在这些连接被关闭之前）。
- **聚合时间间隔** - 指定从端点导出数据流的时间间隔。使用 5 秒默认值时，一个数据包中将捕获不止一个数据流。如果时间间隔值为 0 秒，则每个数据包都有一个数据流。有效范围为 0 到 600 秒。
- **限制速率 (Throttle Rate)** - 限制控制以什么速率将数据从缓存发送到收集器，以便尽量减小对最终用户的影响。您可以对实时和缓存数据应用限制（只要存在缓存的数据）。以 Kbps 为单位，输入限制速率。默认值为 500 Kbps。

  在该固定时段后，缓存数据将被导出。输入 0 将禁用该功能。
- **收集模式 (Collection Mode)** - 通过选择收集模式关闭 (collection mode is off)、仅受信任网络 (trusted network only)、仅不受信任网络 (untrusted network only) 或所有网络 (all networks)，指定应从终端收集数据的时间。
- **收集标准 (Collection Criteria)** - 您可以在数据收集时减少不必要的广播，以便仅分析相关数据。通过以下选项控制数据搜集：
  - **广播数据包 (Broadcast packets)** 和**组播数据包 (Multicast packets)**（仅适用于桌面）- 默认情况下，为了提高效率，会关闭广播和组播数据包收集，以便缩短在后端资源上花费的时间。单击该复选框可启用对广播和组播数据包的收集并过滤数据。
  - **仅限 KNOX (KNOX only)**（可选且特定于移动设备）- 选中后，将仅从 KNOX 工作空间收集数据。默认情况下，未选中此字段，将会从工作空间内部和外部收集数据。
- **数据收集策略 (Data Collection Policy)** - 您可以添加数据收集策略，并将它们与网络类型或连接情形相关联。您可以将一种策略应用于 VPN，而将另一种策略应用于非 VPN 流量，因为多个接口可以同时处于活跃状态。

  在单击“添加”(Add) 时，系统显示“数据收集策略”(Data Collection Policy) 窗口。在创建策略时，请记住以下指导原则：
  - 默认情况下，如果未创建策略或未与网络类型相关联，则将报告和收集所有字段。
  - 每种数据收集策略必须与至少一种网络类型相关联，但您不能将两种策略与同一种网络类型相关联。
  - 具有更具体的网络类型的策略优先。例如，因为 VPN 是受信任网络的一部分，所以包含 VPN 网络类型的策略的优先级高于采用受信任网络为指定网络的策略。
  - 您只能基于所选的收集型号，为网络创建适用的数据收集策略。例如，如果**收集模式 (Collection Mode)** 设置为 **仅受信任网络 (Trusted Network Only)**，您无法为**不受信任网络类型 (Untrusted Network Type)** 创建**数据收集策略 (Data Collection Policy)**。

- 如果从较新版本的 AnyConnect 打开来自较早版本 AnyConnect 的配置文件，它会自动将该配置文件转换为较新的版本。转换过程中会为所有网络添加数据收集策略，用于排除先前匿名的字段。

- **名称 (Name)** - 为您要创建的策略指定名称。

- **网络类型 (Network Type)** - 通过选择 VPN、受信任或不受信任，来确定收集模式，或者应用数据收集策略的网络。如果您选择受信任网络，则策略也适用于 VPN 案例。

- **流过滤器规则** - 定义一组条件和一个操作，可以在满足所有条件时收集或忽略流。您最多可以配置 25 条规则，每条规则最多可以定义 25 个条件。使用“流过滤器规则”列表右侧的向上和向下按钮调整规则的优先级，并对后续规则给予更高的考虑。单击**添加 (Add)** 设置流过滤器规则的组成要素。

  - 名称 - 流过滤器规则的唯一名称。

  - 类型 - 每个过滤器规则都有“收集”或“忽略”类型。确定满足过滤器规则时要执行的操作（“收集”或“忽略”）。如果收集，则在满足条件时允许流。如果忽略，则丢弃流。

  - 条件 - 为要匹配的每个字段添加一个条目以及一个运算，以确定字段值对匹配项是否应相等或不相等。每个运算都有一个字段标识符和该字段的对应值。该字段区分大小写，除非您在设置过滤器引擎规则时对规则集应用了不区分大小写操作 (EqualsIgnoreCase)。启用后，规则中设置的 Value 字段中的输入不区分大小写。

- **包括/排除**

  - **类型 (Type)** - 确定要在数据收集策略中**包含 (Include)** 或**排除 (Exclude)** 的字段。默认值为**排除 (Exclude)**。所有未选中的字段都收集起来。未选中任何字段时，将收集所有字段。

  - **字段** - 确定要从终端接收哪些信息以及收集哪些字段的数据以满足策略要求。根据网络类型和包含或排除的字段，NVM 将在终端上收集相应数据。

注释 升级期间，如果存在以下情况之一，默认从流信息的报告中排除 ProcessPath、ParentProcessPath、ProcessArgs 和 ParentProcessArgs：

- 如果较旧版本NVM中的配置文件没有数据收集策略或有包含数据收集策略。
- 如果较旧版本 NVM 中的配置文件有排除数据收集策略，并且该配置文件已使用更新的4.9版本配置文件编辑器打开并保存。如果较旧版本NVM中的配置文件有排除数据收集策略，但该配置文件未使用更新的4.9版本配置文件编辑器打开和保存，则包含这四个字段。

如果 NVM 无法计算父进程 ID，则值默认为 4294967295。

FlowStartMsec 和 FlowStopMsec 确定流的纪元时间戳（以毫秒为单位）。

对于 AnyConnect 版本4.4（和更高版本），您现在可以选择接口状态和 SSID，这将指定接口的网络状态为受信任还是不受信任。

- **可选匿名字段 (Optional Anonymization Fields)** - 如果要关联同一终端上的记录，同时保留隐私，请选择所需的字段进行匿名化，它们将作为值的哈希而不是实际值进行发送。字段的子集可用于匿名化。

  标记为包含或排除的字段不可用于匿名；同样，标记为匿名的字段不可用于包含或排除。

- **用于 Knox 的数据收集策略 (Data Collection Policy for Knox)**（**特定于移动设备**）- 该选项用于在选择移动配置文件时指定数据收集策略。要为 Knox 容器创建数据收集策略，请选择“范围”(Scope) 下的**仅 Knox (Knox-Only)** 复选框。除非指定单独的 Knox 容器数据收集策略，否则应用于 Knox 容器流量的设备范围内的数据收集策略也适用于 Knox 容器流量。要添加或删除数据收集策略，请参阅上面的数据收集策略说明。您可以为移动配置文件设置最多 6 个不同的数据收集策略：3 个用于设备，3 个用于 Knox。

- **可接受的使用策略 (Acceptable Use Policy)**（可选且特定于移动设备）- 单击**编辑 (Edit)**，在对话框中为移动设备定义可接受的使用策略。完成后，单击**确定 (OK)**。最多允许 4000 个字符。

  配置NVM后，此消息会显示给用户。远程用户无法选择拒绝NVM活动。网络管理员使用MDM工具控制 NVM。

- **Export on Mobile Network**（**可选且特定于移动设备**）- 指定在设备使用移动网络时，是否允许导出 NVM 流。如果启用（默认值），当显示或后续通过 AnyConnect Android 应用中的 **设置 (Settings)** > **NVM-设置 (NVM-Settings)** > > **将移动数据用于 NVM (Use mobile data for NVM)** 复选框来显示“可接受的用户策略”(Acceptable User Policy) 窗口时，最终用户可以覆盖管理员 。如果取消选中“在移动网络上导出”(Export on Mobile Network) 复选框，当设备使用移动网络时，不会导出 NVM 流，最终用户无法对其进行更改。

- **受信任的网络检测** — 此功能可检测终端是否实际上位于企业网络中。NVM 使用网络状态来确定何时导出 NVM 数据并应用相应的数据收集策略。单击**配置 (Configure)** 以设置受信任的网络检测的配置。SSL 探测会发送到已配置的受信任前端，如果可访问，则前端会使用证书响应。然后，系统将根据配置文件编辑器中的散列设置提取指纹（SHA-256 散列）并将其与之匹配。成功匹配表明终端位于受信任的网络中；但是，如果前端无法访问，或者如果证书散列不匹配，则系统会将终端视为位于不受信任的网络中。

  注释 从内部网络的外部进行操作时，TND 会执行 DNS 请求并尝试与已配置服务器建立 SSL 连接。思科强烈建议使用别名，以确保在内部网络以外使用的机器不会通过这些请求泄露您组织的名称和内部结构。

  如果 TND 未在 NVM 配置文件中配置或如果已安装了 VPN 模块，NVM 会使用 配置值得信赖的网络检测来确定终端是否位于受信任的网络中。如果已安装 VPN 模块并在 NVM 配置文件中配置了 TND，则 NVM 会执行值得信赖的网络检测，即使在 VPN 网络内部也是如此。在以前的版本中，VPN 网络会被默认视为受信任的网络。NVM 配置文件编辑器中的 TND 配置包括以下内容：

  1. **https://** — 输入每个受信任服务器的 URL （IP 地址、FQDN 或端口地址），然后单击**添加 (Add)**）。

     注释 代理后的受信任服务器不受支持。

  2. **证书散列 (SHA-256)** — 如果与受信任服务器的 SSL 连接成功，则系统会自动填充此字段。否则，您可以通过输入服务器证书的 SHA-256 散列并单击**设置 (Set)** 来手动对其进行设置。
  3. **受信任服务器列表** — 通过此过程可以定义多个受信任服务器。（至多 10 个。）由于服务器会按已配置的顺序尝试受信任的网络检测，因此您可以使用**上移**和**移动 |向下**按钮来调整该顺序。如果终端无法连接到第一台服务器，它会尝试连接第二台服务器，依此类推。在对列表中的所有服务器进行尝试后，终端等待 10 秒后会再进行最后一次尝试。当服务器进行身份验证时，系统会视为终端在受信任的网络中。

将配置文件另存为 `NVM_ServiceProfile.xml`。您必须将配置文件准确保存为此名称，否则NVM 将无法收集和发送数据。

AnyConnect 本地策略

AnyConnectLocalPolicy.xml 是包含安全设置的客户端上的 XML 文件。ASA 不部署该文件。您必须使用企业软件部署系统手动安装该文件或将其部署到用户计算机中。如果您对用户系统中的现有本地策略文件进行了更改，则系统将重启。

本地策略首选项

您可以在 VPN 本地策略编辑器中指定要包含在 `AnyConnectLocalPolicy.xml` 文件中的以下首选项。

- **FIPS 模式**

  为客户端启用 FIPS 型号。此设置强制客户端仅使用 FIPS 标准批准的算法和协议。

- **旁路下载程序**

  选择后，禁用 VPNDownloader.exe 模块启动，该模块负责检测本地版本动态内容的存在和更新。客户端不检查 ASA 上的动态内容，包括转换、定制、可选模块和核心软件更新。

  选中“旁路下载程序”(Bypass Downloader) 时，在客户端连接到 ASA 时将发生两种情况之一：

  - 如果 ASA 上的 VPN 客户端配置文件不同于客户端上的 VPN 客户端配置文件，则客户端将中止连接尝试。
  - 如果 ASA 上没有 VPN 客户端配置文件，则客户端会建立 VPN 连接，但它使用其硬编码的 VPN 客户端配置文件设置。

  注释 如果您在 ASA 上配置 VPN 客户端配置文件，则这些文件必须在客户端连接到 ASA 之前安装在客户端上（BypassDownloader 设置为 true）。因为配置文件可以包含管理员定义的策略，所以只在您不依赖于 ASA 来集中管理客户端配置文件时，才建议将 BypassDownloader 设置为 true。

- **启用 CRL 检查**

  仅对 *Windows* 桌面实施此功能。对于 SSL 和 IPsec VPN 连接，可以选择执行证书吊销列表 (CRL) 检查。启用此设置后，AnyConnect 检索链中所有证书的已更新 CRL。然后，AnyConnect 验证有关证书是否包含在不应再信任的这些已吊销证书中。如果发现该证书已被证书颁发机构 (CA) 吊销，则不进行连接。

  默认情况下会禁用 CRL 检查。仅当选中（或启用）“启用 CRL 检查”(Enable CRL Check) 时，AnyConnect 才会执行 CRL 检查，因此，最终用户可能会观察到以下情况：

  - 如果通过 CRL 吊销证书，即使在 AnyConnect 本地策略文件中禁用 Strict Certificate Turst，与安全网关的连接也会无条件失败。
  - 如果无法检索 CRL（例如由于无法访问 CRL 分发点），并且在 AnyConnect 本地策略文件中启用 Strict Certificate Turst，与安全网关的连接也会无条件失败。否则，如果禁用 Strict Certificate Turst，则系统可能会提示该用户绕过此错误。

注释 启用 Always On 时，AnyConnect 无法执行 CRL 检查。此外，如果 CRL 分发点不是公开可访问，则 AnyConnect 可能会遇到服务中断。

- **启用 OCSP 检查**

  此功能仅对 *Linux* 实施。它让客户端可以实时查询各个证书的状态，具体方法为：向 OSCP 响应程序发送请求，并解析 OSCP 响应，即可获得证书状况。OCSP 用于验证整个证书链，并且仅与 PEM 文件证书存储库配合使用（通过将 Exclude Firefox NSS Cert Store 设置为 *True*）。对于每个证书，访问 OCSP 响应程序设有五秒的超时间隔。

  默认情况下会禁用 OCSP 检查。如已启用，最终用户可能会观察到以下情况：

  - 如果通过 OCSP 吊销证书，即使在 AnyConnect 本地策略文件中禁用 Strict Certificate Turst，与网关的连接也会无条件失败。
  - 如果无法连接到 OCSP，并且在 AnyConnect 本地策略文件中启用 Strict Certificate Turst，与安全网关的连接也会无条件失败。否则，如果禁用 Strict Certificate Turst，则系统可能会提示该用户绕过此错误。

  注释 启用“永远在线”(Always On) 后，AnyConnect 将无法执行 OCSP 检查。此外，如果 OCSP 响应程序并非可公开访问，则 AnyConnect 可能会遇到服务中断。

- **限制 Web 启动**

  阻止用户使用不符合 FIPS 的浏览器来发起 WebLaunch。其实现途径是阻止客户端获取用于发起 AnyConnect 隧道的安全 Cookie。客户端向用户显示一条信息性消息。

- **严格证书信任**

  如果选中此项，则在对远程安全网关进行身份验证时，AnyConnect 不允许它无法验证的任何证书。客户端并不提示用户接受这些证书，而是无法使用自签证书连接到安全网关并显示本地策略禁止接受不受信任的服务器证书。不会建立连接。。如果未选中，客户端将提示用户接受证书。这是默认行为。

  我们强烈建议您为 AnyConnect 客户端启用“严格证书信任”，原因如下：

  - 随着有针对性攻击的日益增多，在本地策略中启用 Strict Certificate Turst 有助于在用户从不受信任网络（例如公共访问网络）连接时，防止受到“中间人”攻击。
  - 即使您使用完全可验证且受信任的证书，默认情况下 AnyConnect 客户端也允许最终用户接受不可验证的证书。如果最终用户受到中间人攻击，他们可能会被提示接受恶意证书。要从最终用户删除此决定，请启用 Strict Certificate Turst。

- **限制服务器证书存储库**（Windows、macOS 和 Linux）

防止客户端使用基于用户的证书存储验证服务器证书。只使用基于系统的证书存储。启用此项还将启用 <StrictCertificateTrust> 并将其设置为 true。

- **限制首选项缓存**

  根据设计，AnyConnect 不将敏感信息缓存到磁盘。启用此参数会将本策略扩展到在 AnyConnect 首选项中存储的任何类型的用户信息。

  - Credentials - 不缓存用户名和辅助用户名。
  - Thumbprints - 不缓存客户端和服务器的证书拇指指纹。
  - CredentialsAndThumbprints - 不缓存证书拇指指纹和用户名。
  - All - 不缓存任何自动首选项。
  - false - 所有首选项都写入磁盘（默认值）。

- **限制网络部署更新—**

  注释 通过升级到 AnyConnect 4.10（或更高版本），您可以选择按照此处的定义来配置完全限制。但是，您可以通过创建受信任 ASA 列表并选择从这些受信任 ASA 下载策略、帮助文件、转换和脚本，改为将下载程序分发仅限制为受信任的 ASA 源。请参阅下面的“更新策略参数”。

  以下设置允许您绕过某些下载程序功能，同时保留 VPN 配置文件更新和软件更新功能。您可以通过 ASA 禁用脚本、本地化文件、帮助文件或用户界面自定义的 Web 部署，而不会影响 AnyConnect 下载程序的其他功能。如果设置为绕过，则必须使用带外软件更新机制来完成任何必要的更新。

  - **限制脚本 Web 部署更新 (Restrict Script Web-deploy Updates)** - 防止管理员从服务器自定义连接脚本更新。
  - **限制资源 Web 部署更新 (Restrict Resource Web-deploy Updates)**- 防止管理员从服务器自定义用户界面元素更新。
  - **限制帮助 Web 部署更新 (Restrict Help Web-deploy Updates)** - 防止管理员从服务器自定义帮助文件更新。
  - **限制本地化 Web 部署更新 (Restrict Localization Web-deploy Updates)** - 防止管理员从服务器自定义本地化更新。

- **排除 PEM 文件证书存储库 (Exclude Pem File Cert Store)**（Linux 和 macOS）

  防止客户端使用 PEM 文件证书存储库来验证服务器证书和搜索客户端证书。

  存储库使用支持 FIPS 的 OpenSSL，并具有关于在哪里可以获取客户端证书身份验证所需证书的信息。允许 PEM 文件证书存储库可确保远程用户使用符合 FIPS 的证书存储库。

- **排除 Firefox NSS 证书存储区库 (Exclude Firefox NSS Cert Store)** (Linux)

防止客户端使用 Firefox NSS 证书存储库来验证服务器证书和搜索客户端证书。

存储库有关于在何处为客户端证书身份验证取得证书的信息。

- 更新策略

  控制客户端可以从哪些前端获取软件或配置文件更新。默认情况下，允许将来自任何服务器的更新设置为 *TRUE*。要将下载程序分发仅限于受信任的ASA源，请在“服务器名称”(Server Name) 字段中添加服务器名称，并取消选中您不希望允许的服务器更新。在 AnyConnect 4.10 之前的版本中，“允许软件更新”(Allow Software Updates) 包含脚本、帮助文件、资源和本地化，这些是四个单独的设置。

  - **Allow Software Updates From Any Server**
  - **Allow Compliance Module Updates From Any Server**（允许任何服务器的合规模块更新）
  - **Allow VPN Profile Updates From Any Server**
  - **Allow Management VPN Profile Updates From Any Server**（允许任何服务器的 VPN 配置文件更新）
  - **Allow ISE Posture Profile Updates From Any Server**（允许任何服务器的 ISE 终端安全评估配置文件更新）
  - **Allow Service Profile Updates From Any Server**
  - **允许任何服务器的脚本更新 (Allow Script Updates From Any Server)**
  - **Allow Help Updates From Any Server**（允许任何服务器的帮助更新）
  - **允许任何服务的软件更新 (Allow Software Updates From Any Server)**
  - **允许任何服务的本地化更新 (Allow Localization Updates From Any Server)**
  - 服务器名称

    在此列表中指定已授权服务器。允许这些前端在建立 VPN 连接后进行所有 AnyConnect 软件和配置文件的完全更新。服务器名称可以是 FQDN、IP 地址、域名或通配符加域名。

- **受信任的 ISE 证书指纹 (SHA256) (Trusted ISE Certificate Fingerprints [SHA256])** - 允许您在获取终端安全评估策略之前建立 ISE 信任。您可以在 ISE 认证链中指定 ISE 证书、中间 CA 证书或根 CA 证书的 SHA256 指纹。SHA256 指纹区分大小写，添加时可使用也可不使用冒号。该设置对于脚本补救是必不可少的。

在 MST 文件中启用本地策略参数

有关说明和可以设置的值，请参阅本地策略首选项。

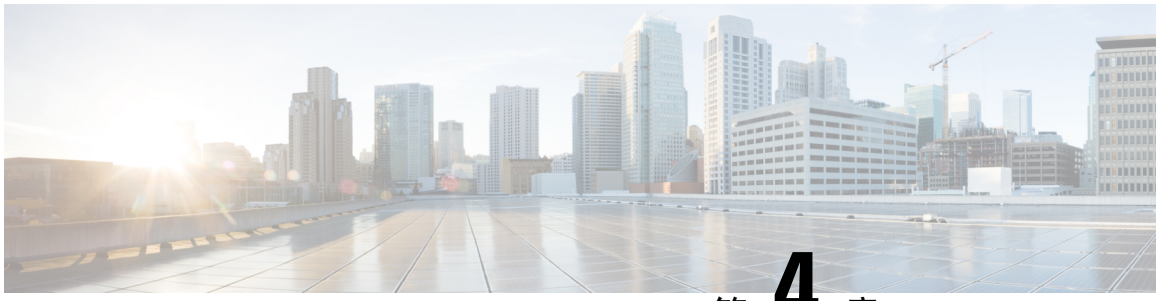
创建 MST 文件以更改本地策略参数。MST 参数名称对应于 AnyConnect 本地策略文件 (AnyConnectLocalPolicy.xml) 中的参数：

- LOCAL_POLICY_BYPASS_DOWNLOADER

- LOCAL_POLICY_FIPS_MODE
- LOCAL_POLICY_RESTRICT_PREFERENCE_CACHING
- LOCAL_POLICY_RESTRICT_TUNNEL_PROTOCOLS
- LOCAL_POLICY_RESTRICT_WEB_LAUNCH
- LOCAL_POLICY_STRICT_CERTIFICATE_TRUST

注释 AnyConnect 安装不会自动覆盖用户计算机上的现有本地策略文件。必须先删除用户计算机上的现有策略文件，以便客户端安装程序可以创建新的策略文件。

注释 对本地策略文件的任何更改都需要重新启动系统。



第 4 章

配置 VPN 访问

连接和断开 VPN

AnyConnect VPN 连接选项

AnyConnect 客户端为自动连接、自动重新连接或自动断开 VPN 会话提供多种选项。这些选项方便用户连接您的 VPN，它们还支持您的网络安全要求。

启动和重新启动 AnyConnect 连接

配置 VPN 连接服务器为您的用户所要手动连接的安全网关提供名称和地址。

选择以下 AnyConnect 功能，以提供方便的自动 VPN 连接：

- 登录前自动启动 Windows VPN 连接
- AnyConnect 启动时自动启动 VPN 连接
- 自动重新启动 VPN 连接

此外，还应考虑使用以下自动 VPN 策略选项实施增强的网络安全或将网络访问仅限于 VPN：

- 关于值得信赖的网络检测

- 需要使用 永远在线 的 VPN 连接
- 使用强制网络门户热点检测和补救

重新协商和维护 AnyConnect 连接

您可以限制 ASA 对用户保持 AnyConnect VPN 连接的时间长度（即便没有活动）。如果 VPN 会话进入空闲状态，您可以终止连接或重新协商连接。

- Keepalive - ASA 定期发送保持连接消息。这些消息会被 ASA 忽略，但对于维持客户端与 ASA 之间设备的连接很有用。

  有关通过 ASDM 或 CLI 配置保持连接的说明，请参阅思科 ASA 系列 VPN 配置指南中的启用保持连接部分。

- Dead Peer Detection - ASA 和 AnyConnect 客户端发送“R-U-There”消息。这些消息的发送频率低于 IPsec 的保持连接消息。您可以同时启用 ASA（网关）和 AnyConnect 客户端来发送 DPD 消息，并配置超时间隔。
  - 如果客户端未响应 ASA 的 DPD 消息，ASA 将再重试一次才将会话置于 Waiting to Resume 型号。此型号可使用户漫游网络，或进入睡眠型号，然后恢复连接。如果用户在空闲超时之前没有重新连接，ASA 将终止隧道。建议的网关 DPD 间隔是 300 秒。
  - 如果 ASA 不响应客户端的 DPD 消息，客户端将再尝试一次才终止隧道。建议的客户端 DPD 间隔是 30 秒。

    有关在 ASDM 中配置 DPD 的说明，请参阅相应版本的思科 ASA 系列 VPN 配置指南中的配置失效对等点检测。

- 最佳实践：
  - 将客户端 DPD 设置为 30 秒 (Group Policy > Advanced > AnyConnect Client > Dead Peer Detection)。
  - 将服务器 DPD 设置为 300 秒 (Group Policy > Advanced > AnyConnect Client > Dead Peer Detection)。
  - 将 SSL 和 IPsec 的密钥重新生成均设置为 1 小时 (Group Policy > Advanced > AnyConnect Client > Key Regeneration)。

终止 AnyConnect 连接

终止 AnyConnect 连接要求用户在安全网关上对其终端设备重新进行身份验证，并创建新的 VPN 连接。

以下连接参数基于超时终止 VPN 会话：

- Maximum Connect Time - 设置用户最长连接时间（以分钟为单位）。此时间结束时，系统会终止连接。您还可以允许无限连接时间（默认）。

- VPN Idle Timeout - 当会话处于非活动状态达到指定的时间时，终止任何用户会话。如果未配置 VPN 空闲超时，则使用默认空闲超时。
- Default Idle Timeout - 当会话处于非活动状态达到指定的时间时，终止任何用户会话。默认值为 30 分钟。默认值为 1800 秒。

请参阅相应版本的思科 ASA 系列 VPN 配置指南中的指定组策略的 *VPN* 会话空闲超时部分。

配置 VPN 连接服务器

AnyConnect VPN 服务器列表包含主机名和主机地址对，它们标识 VPN 用户将连接到的安全网关。主机名可以是别名、FQDN 或 IP 地址。

添加到服务器列表的主机显示在 AnyConnect GUI 的 Connect to 下拉列表中。然后，用户可以从下拉列表中进行选择以发起 VPN 连接。列表顶部的主机是默认服务器，在 GUI 下拉列表中首先出现。如果用户从列表中选择备用服务器，则所选服务器成为新的默认服务器。

一旦您将服务器添加到服务器列表，就可以查看其详细信息以及编辑或删除服务器条目。要将服务器添加到服务器列表，请遵循此过程。

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择**服务器列表 (Server List)**。

步骤 2 单击**添加 (Add)**。

步骤 3 配置服务器的主机名和地址：

a) 输入 **Host Display Name**、用于指代主机的别名、FQDN 或 IP 地址。请勿在名称中使用“&”或“<”字符。如果您输入 FQDN 或 IP 地址，则无需在下一步骤中输入 **FQDN** 或 **IP Address**。

如果输入 IP 地址，请使用安全网关的公共 IPv4 地址或全局 IPv6 地址。不支持使用链路本地安全网关地址。

b) （可选）输入主机的 **FQDN** 或 **IP Address**（如果在 Host Display Name 中没有输入）。

c) （可选）指定 **User Group**。

AnyConnect 使用 FQDN 或 IP 地址以及用户组来构成组 URL。

步骤 4 在 **Backup Server List** 中输入要回退到作为备用服务器的服务器。请勿在名称中使用“&”或“<”字符。

注释 相反，“服务器”(Server) 菜单上的“备份服务器”(Backup Server) 选项卡是所有连接条目的全局条目。将使用在此处为单个服务器列表条目输入的条目覆盖放入备用服务器位置中的任何条目。此设置优先，并且是推荐做法。

步骤 5 （可选）将负载均衡服务器添加到**负载均衡服务器列表.**。请勿在名称中使用“&”或“<”字符。

如果此服务器列表条目的主机指定安全设备的负载均衡集群，且启用了 永远在线 功能，请将集群中的负载均衡设备添加到此列表中。否则，永远在线 将阻止访问负载均衡集群中的设备。

步骤 6 为客户端指定 **Primary Protocol** 以用于此 ASA：

a) 选择 SSL（默认值）或 IPsec。

如果您指定 IPsec，则用户组必须是连接配置文件（隧道组）的准确名称。对于 SSL，用户组是连接配置文件的组 URL 或组别名。

b) 如果您指定 IPsec，请选择**仅标准身份验证 (Standard Authentication Only)** 以禁用默认身份验证方法（专有 AnyConnect EAP），然后从下拉列表中选择一种方法。

注释 将身份验证方法从专有的 AnyConnect EAP 更改为基于标准的方法会禁用 ASA 配置会话超时、空闲超时、连接断开超时、分割隧道、分离 DNS、MSIE 代理配置及其他功能的能力。

步骤 7 （可选）为此服务器配置 SCEP：

a) 指定 SCEP CA 服务器的 URL。输入 FQDN 或 IP 地址。例如，http://ca01.cisco.com。

b) 选中**提示质询密码 (Prompt For Challenge PW)** 以让用户手动发出证书请求。当用户单击**获取证书 (Get Certificate)** 时，客户端将提示用户输入用户名和一次性密码。

c) 输入 CA 的证书拇指指纹。使用 SHA1 或 MD5 哈希值。您的 CA 服务器管理员可以提供 CA URL 和拇指指纹，且应该直接从服务器（而不是发布证书的 fingerprint 或 thumbprint 属性字段）检索拇指指纹。

步骤 8 单击**确定 (OK)**。

相关主题

AnyConnect 配置文件编辑器，服务器列表，第 89 页
AnyConnect 配置文件编辑器，添加/编辑服务器列表，第 90 页

登录前自动启动 Windows VPN 连接

关于“登录前启动”

登录前启动 (SBL) 这一功能允许用户在登录 Windows 之前建立与企业基础设施的 VPN 连接。

注释 使用登录前启动 (SBL) 和 HostScan 时，因为 SBL 是预登录，所以必须在终端上安装 AnyConnect/HostScan 安全评估预部署模块才能实现完整的 HostScan 功能。

在安装并启用 SBL 后，网络连接 (Network Connection) 按钮用于启动 AnyConnect VPN 和网络接入管理器 UI。

SBL 还包括网络访问管理器图块，允许使用用户配置的家庭网络配置文件进行连接。SBL 型号中允许的网络配置文件包括使用非 802-1X 身份验证型号的所有媒体类型，例如开放 WEP、WPA/WPA2 个人和静态密钥 (WEP) 网络。

SBL 仅在 Windows 系统中可用，并使用取决于 Windows 版本的不同机制来实施：

- 在 Windows 中，登录前访问提供商 (PLAP) 用于实施 AnyConnect SBL。

  使用 PLAP 时，按 Ctrl+Alt+Del 组合键后打开一个窗口，在这个窗口中用户可以选择登录到系统或使用窗口右下角的“网络连接”(Network Connect) 按钮来激活网络连接（PLAP 组件）。

  PLAP 支持 Windows 的 32 位和 64 位版本。

您应该考虑为用户启用 SBL 的原因包括：

- 用户的计算机加入 Active Directory 基础设施。
- 用户拥有要求使用 Microsoft Active Directory 基础设施进行身份验证的网络映射驱动器。
- 用户无法在计算机上缓存凭证（组策略禁止缓存凭证）。在这种情况下，用户必须能够与企业网络中的域控制器通信，以便在获得计算机访问权限之前对其凭证进行验证。
- 用户必须运行从网络资源执行的登录脚本或需要访问网络资源。SBL 处于启用状态时，用户可访问本地基础设施和用户在办公室时通常会运行的登录脚本。这包括域登录脚本、组策略对象和用户登录其系统时通常发生的其他 Active Directory 功能。
- 存在可能需要连接到基础设施的网络组件（例如 MS NAP/CS NAC）。

“登录前启动”的限制

- AnyConnect 不与快速用户切换兼容。
- AnyConnect 无法由第三方登录前启动应用程序启动。

配置登录前启动

步骤 1 安装 AnyConnect 登录前启动模块。

步骤 2 在 AnyConnect 配置文件中启用 SBL。

安装 AnyConnect 登录前启动模块

AnyConnect 安装程序会检测基础操作系统，并将来自 AnyConnect SBL 模块的适当 AnyConnect DLL 置于系统目录中。在 Windows 7 或 Windows 2008 服务器上，安装程序会确定正在使用的是 32 位还是 64 位版本的操作系统，并安装适当的 PLAP 组件，即 vpnplap.dll 或 vpnplap64.dll。

注释 如果在保留已安装的 SBL 模块的情况下卸载 AnyConnect，SBL 模块会禁用且远程用户看不见该组件。

您可以预部署 SBL 模块或配置 ASA 以下载 SBL 模块。预部署 AnyConnect 时，登录前启动模块会要求先安装核心客户端软件。如果使用 MSI 文件预部署 AnyConnect 核心和登录前启动组件，则必须按照正确的顺序进行操作。

步骤 1 在 ASDM 中，转到**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **组策略 (Group Policies)**。

步骤 2 选择组策略，单击**编辑 (Edit)** 或**添加 (Add)** 可编辑或新增组策略。

步骤 3 在左侧导航窗格中选择**高级 (Advanced)** > **AnyConnect 客户端 (AnyConnect Client)**。

步骤 4 对“用于下载的可选客户端模块”(Optional Client Module for Download) 设置取消选中**继承 (Inherit)**。

步骤 5 在下拉列表中选择 **AnyConnect SBL** 模块。

在 AnyConnect 配置文件中启用 SBL

开始之前

- 在调用 SBL 时需要存在网络连接。但在有些情况下，网络连接可能无法实现，因为无线连接可能依靠用户凭证才能连接到无线基础设施。由于 SBL 型号先于登录的凭证阶段存在，因此此情况下连接不可用。此时，无线连接需要配置为在登录过程中缓存凭证，或者需要配置其他无线身份验证，SBL 才可正常运行。
- 如果安装了网络访问管理器，您必须部署设备连接以确保适当的连接可用。

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择**首选项（部分 1）(Preferences [Part 1])**。

步骤 2 选择**使用登录前启动 (Use Start Before Login)**。

步骤 3 （可选）要允许远程用户控制 SBL，请选择**用户可控制 (User Controllable)**。

注释　在 SBL 生效之前，用户必须重新启动远程计算机。

登录前启动故障排除

步骤 1 确保 AnyConnect 配置文件已载入 ASA 上，随时可部署。

步骤 2 删除之前的配置文件（在硬盘驱动器上搜索这些文件以找到位置，*.xml）。

步骤 3 使用 Windows Add/Remove Programs 卸载 SBL 组件。重新启动计算机并重新测试。

步骤 4 在事件查看器中清除用户的 AnyConnect 日志并重新测试。

步骤 5 浏览回安全设备以再次安装 AnyConnect。

步骤 6 重新启动一次。下次重新启动时，您应看到“登录前启动”(Start Before Login) 提示。

步骤 7 收集 DART 捆绑包并将其发送给 AnyConnect 管理员。

步骤 8 如果看到以下错误，请删除用户的 AnyConnect 配置文件：

```
Description: Unable to parse the profile C:\Documents and Settings\All Users\Application Data
\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\VABaseProfile.xml. Host data not available.
```

步骤 9 返回 .tmpl 文件，将副本另存为 .xml 文件，并将该 XML 文件用作默认配置文件。

AnyConnect 启动时自动启动 VPN 连接

此功能称为 Auto Connect On Start，它在 AnyConnect 启动时自动与 VPN 客户端配置文件指定的安全网关建立 VPN 连接。

“启动时自动连接”(Auto Connect On Start) 默认禁用，需要用户指定或选择安全网关。

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择**首选项（部分 1）(Preferences [Part 1])**。

步骤 2 选择**启动时自动连接 (Auto Connect On Start)** 。

步骤 3 （可选）要让用户控制“启动时自动连接”(Auto Connect On Start)，请选择**用户可控制 (User Controllable)**。

在 Windows 系统上配置登录前启动 (PLAP)

登录前启动 (SBL) 功能在用户登录到 Windows 之前启动一个 VPN 连接。这将确保用户在登录到计算机之前连接其公司基础设施。Windows 仅支持一次安装一个 PLAP。

SBL AnyConnect 功能称为登录前接入提供商 (PLAP)，它是一个可连接的凭证提供商。此功能可让编程网络管理员在登录前执行特定的任务，如收集凭证或连接到网络资源。PLAP 在所有受支持的 Windows 操作系统上提供 SBL 功能。PLAP 分别以 vpnplap.dll 和 vpnplap64.dll 支持 32 位和 64 位版本的操作系统。PLAP 功能支持 x86 和 x64。

自动重新启动 VPN 连接

启用 Auto Reconnect（默认值）时，AnyConnect 将从 VPN 会话中断中恢复并重新建立会话，而不管初始连接使用哪种介质。例如，它可以重新建立有线、无线或3G会话。启用“自动重新链接”后，您还可以指定系统暂停或系统恢复时的重新连接行为。系统暂停是低功耗待机状态，如 Windows 的“休眠”或者 macOS 或 Linux 的“睡眠”。系统恢复是系统暂停后的恢复。

如果禁用 Auto Reconnect，无论连接出于何种原因断开，客户端都不会尝试重新连接。思科强烈建议对此功能使用默认设置（启用）。禁用此设置可能导致连接不稳定时 VPN 连接中断。

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择**首选项（部分 1）(Preferences [Part 1])**。

步骤 2 选择**自动重新连接 (Auto Reconnect)**。

步骤 3 选择“自动重新连接行为”(Auto Reconnect Behavior)：

- Disconnect On Suspend -（默认值）AnyConnect 在系统暂停时释放分配给 VPN 会话的资源，并且在系统恢复后不尝试重新连接。
- Reconnect After Resume - 客户端在系统暂停期间保留分配给 VPN 会话的资源，并且在系统恢复后尝试重新连接。

使用值得信赖的网络检测来连接和断开连接

关于值得信赖的网络检测

值得信赖的网络检测 (TND) 可让您在用户处于企业网络（值得信赖的网络）内时让 AnyConnect 自动断开 VPN 连接，并在用户处于企业网络（不值得信赖的网络）之外时启动 VPN 连接。

TND 不会影响用户手动建立 VPN 连接的能力。它不会断开用户在值得信赖的网络中手动启动的 VPN 连接。如果用户先在不值得信赖的网络中，然后进入值得信赖的网络，TND 只断开 VPN 会话的连接。举例来说，如果用户在家建立 VPN 连接，然后移动到公司办公室，则 TND 会断开 VPN 会话的连接。

注释 要为 Network Visibility Module 配置 TND 功能，请参阅 " *Network Visibility Module* " 一章的 NVM 配置文件编辑器 ， 第 94 页。

您可以在 AnyConnect VPN 客户端配置文件中配置 TND。不需要更改 ASA 配置。您需要指定 AnyConnect 识别出正在值得信赖的网络和不值得信赖的网络之间过渡时应采取的措施或策略，并确定值得信赖的网络和服务器。

值得信赖的网络检测指南

- 因为 TND 功能控制 AnyConnect GUI 并自动启动连接，所以 GUI 应该始终运行。如果用户退出 GUI，则 TND 不会自动启动 VPN 连接。
- 如果 AnyConnect 也在运行“登录前启动”，且用户进入受信任网络，则计算机上显示的 SBL 窗口将自动关闭。
- 无论是否配置了 永远在线，在通过 IPv4 和 IPv6 网络到 ASA 的 IPv6 和 IPv4 VPN 连接上都支持值得信赖的网络检测。
- 如果 TND 配置不同，在用户计算机上的多个配置文件可能会出现问题。

  如果用户收到过已启用 TND 的配置文件，则系统重新启动时，AnyConnect 会尝试连接它最后一次连接到的安全设备，而这可能不是您希望的行为。要连接到其他安全设备，用户必须手动断开连接并重新连接到该前端。以下解决方法将帮助您避免发生此问题：

  - 在已载入您企业网络中所有 ASA 上的客户端配置文件中启用 TND。
  - 创建一个配置文件（在其主机条目中列出所有 ASA），并将该配置文件载入所有 ASA 上。
  - 如果用户不需要多个不同的配置文件，请为所有 ASA 上的配置文件使用相同的配置文件名称。每个 ASA 都会覆盖现有配置文件。

- 要在 Linux 上使用 TND，您必须在目标 (RHEL/Ubuntu) 设备上安装并正常运行网络管理器，且网络管理器必须维护网络接口。

配置值得信赖的网络检测

步骤 1 打开 VPN 配置文件编辑器，并从导航窗格中选择**首选项（第 2 部分）(Preferences [Part 2])**。

步骤 2 选择**自动 VPN 策略 (Automatic VPN Policy)**。

步骤 3 在**受信任的网络策略 (Trusted Network Policy)** 中选择一个受信任网络策略。

这是用户处于企业网络（受信任网络）中时客户端执行的操作。选项有：

- Disconnect -（默认值）客户端终止受信任网络中的 VPN 连接。
- Connect - 客户端启动受信任网络中的 VPN 连接。
- Do Nothing - 客户端不在受信任网络中执行任何操作。将 Trusted Network Policy 和 Untrusted Network Policy 都设置为 Do Nothing 会禁用 Trusted Network Detection (TND)。
- Pause - 如果用户在受信任网络外建立 VPN 会话之后进入被配置为受信任的网络，则 AnyConnect 会暂停此 VPN 会话而不是将其断开连接。当用户再次离开受信任网络时，AnyConnect 会恢复该会话。此功能是为了给用户提供方便，因为有了它，在用户离开受信任网络后不需要建立新的 VPN 会话。

步骤 4 在**不受信任网络策略 (Untrusted Network Policy)** 中选择一个不受信任的网络策略。

这是用户在企业网络之外时客户端执行的操作。选项有：

- Connect - 客户端在检测到不受信任网络后启动 VPN 连接。
- Do Nothing - 客户端在检测到不受信任网络后不执行任何操作。此选项禁用 永远在线 VPN。将 Trusted Network Policy 和 Untrusted Network Policy 都设置为 **Do Nothing** 会禁用 Trusted Network Detection。

步骤 5 指定 **Trusted DNS Domains**。

指定客户端在信任网络中时网络接口可能具有的 DNS 后缀（逗号分隔的字符串）。如果您将多个 DNS 后缀添加到拆分 DNS 列表并在 ASA 上指定一个默认域，则可以分配多个 DNS 后缀。

AnyConnect 客户端按以下顺序构建 DNS 后缀列表：

- 前端传输的域。
- 前端传输的拆分 DNS 后缀列表。
- 公共接口的 DNS 后缀（如果已配置）。否则，是主后缀和连接特定后缀，以及主 DNS 后缀的父后缀（如果在“高级 TCP/IP 设置”(Advanced TCP/IP Settings) 中选中了相应的复选框）。

要匹配此 **DNS** 后缀，请执行以下操作：	将此值用于 **TrustedDNSDomains**：
example.com（仅限）	*example.com
example.com AND anyconnect.example.com	*.example.com OR example.com, anyconnect.example.com
asa.example.com AND anyconnect.example.com	*.example.com OR asa.example.com, anyconnect.example.com

步骤 6 在 **Trusted DNS Servers** 中指定受信任的 DNS 服务器。

客户端在受信任网络中时网络接口可能具有的所有 DNS 服务器地址（逗号分隔的字符串）。例如：203.0.113.1,2001:DB8::1。IPv4 和 IPv6 DNS 服务器地址支持通配符 (*)。

您必须具有通过 DNS 可解析的前端服务器的 DNS 条目。如果按 IP 地址连接，则需要可以解析 mus.cisco.com 的 DNS 服务器。如果通过 DNS 无法解析 mus.cisco.com，则强制网络门户检测不会按预期工作。

注释 您可以配置 TrustedDNSDomains 和/或 TrustedDNSServers。如果配置 TrustedDNSServers，请确保输入所有 DNS 服务器，这样您的站点会成为受信任网络的一部分。

如果某个活动接口匹配 VPN 配置文件中的所有规则，则将其视为在受信任网络中。

步骤 7 指定一个您要添加为可信 URL 的主机 URL。可信 URL 要求必须存在一个安全 Web 服务器，且可通过可信任证书对其进行访问。在单击**添加 (Add)** 后，将会添加 URL 并预填充证书哈希值。如果未找到哈希值，系统将显示一条错误消息，提示用户手动输入证书哈希值并单击**设置 (Set)**。

注释 只有当一个或以上的受信任的 DNS 域或 DNS 服务器被定义时，您才可以配置该参数。如果受信任的 DNS 域或 DNS 服务器未被定义，则该字段将被禁用。

需要使用 永远在线 的 VPN 连接

关于永远在线 VPN

永远在线 除非 VPN 会话处于活动状态，否则计算机不在受信任网络中时，操作将阻止对互联网资源的访问。在此情况下，始终将 VPN 设置为开启可保护计算机免受安全威胁。

启用了永远在线时，它在用户登录并检测到不受信任网络后自动建立 VPN 会话。VPN 会话保持打开状态，直到用户从计算机中注销，或者会话计时器或空闲会话计时器（在ASA组策略中指定）到期为止。AnyConnect连续尝试重新建立连接以重新激活会话（如果它仍然打开）；否则，它连续尝试建立新 VPN 会话。

在 VPN 配置文件中启用了永远在线时，AnyConnect 可通过删除其他所有下载的 AnyConnect 配置文件并忽略配置为连接到 ASA 的所有公共代理来保护终端。

启用永远在线时，还需要考虑以下 AnyConnect 选项：

- 允许用户将永远在线 VPN 会话断开连接 (Allowing the user to disconnect the 永远在线 VPN session)：AnyConnect 使用户可以将 永远在线 VPN 会话断开连接。如果启用 **Allow VPN Disconnect**，则 AnyConnect 在 VPN 会话建立后显示“断开连接”按钮。默认情况下，启用了永远在线 VPN 时，配置文件编辑器启用 Disconnect 按钮。

  按“断开连接”(Disconnect) 按钮将锁定所有接口以防止数据泄漏以及保护计算机免受互联网访问（除非为了建立 VPN 会话）。永远在线 VPN 会话的用户可能希望单击“断开连接”(Disconnect)，这样，在当前VPN会话出现性能问题或VPN会话中断后的重新连接问题时，他们可以选择备用安全网关。

- 设置连接失败策略 (Setting a connect failure policy)：如果永远在线 VPN 已启用且 AnyConnect 无法建立VPN会话，则连接失败策略将确定计算机是否可以访问互联网。请参阅为永远在线设置连接失败策略。
- 处理强制网络门户热点 (Handling captive portal hotspots)：请参阅使用强制网络门户热点检测和补救。
- 允许在 VPN 断开连接时访问特定主机 (Allowing access to certain hosts while VPN is disconnected)：随**允许在 VPN 断开连接时访问以下主机 (Allow access to the following hosts with VPN disconnected)** 提供的可选配置（某些 HostScan 部署可能需要），当 VPN 在永远在线期间断开连接时，此项将允许终端访问已配置的主机。值是主机的逗号分隔列表，可以是指定 IP 地址、IP 地址范围（CIDR 格式）或 FQDN。最多允许使用 500 个字符。

永远在线 VPN 的限制

- “Always On”（永远在线）仅在 Windows 和 macOS 上可用
- 如果启用了永远在线，但用户没有登录，则 AnyConnect 不建立 VPN 连接。AnyConnect 仅在登录后启动 VPN 连接。
- 永远在线 VPN 不支持通过代理进行连接。

永远在线 VPN 指引

为增强威胁防范，如果您配置了永远在线 VPN，我们建议采取以下额外保护措施：

- 我们强烈建议从证书颁发机构 (CA) 购买数字证书并在安全网关上注册。ASDM 在 **Configuration > Remote Access VPN > Certificate Management > Identity Certificates** 面板上提供一个 **Enroll ASA SSL VPN with Entrust** 按钮，以方便公共证书注册。
- 向终端预部署一个配置有永远在线的配置文件，以限制只能连接到预定义的 ASA。预部署可以防止与欺诈服务器联系。
- 限制管理员权限，以便用户无法终止进程。具有管理权限的 PC 用户可以通过停止代理而忽略永远在线策略。如果想要确保永远在线绝对安全，您必须拒绝给用户分配本地管理权限。
- 限制对 Windows 计算机上思科子文件夹的访问，通常是 `C:\ProgramData`。
- 具有有限或标准权限的用户有时可能对其程序数据文件夹具有写访问权限。他们可以利用这种访问权限删除 AnyConnect 配置文件，从而避开 永远在线 功能。
- 为 Windows 用户预部署一个组策略对象 (GPO)，以防止具有有限权限的用户终止 GUI。为 macOS 用户预部署等效措施。

配置永远在线 VPN

步骤 1 在 AnyConnect VPN 客户端配置文件中配置永远在线，第 116 页。
步骤 2 （可选）向服务器列表添加负载均衡备用集群成员。
步骤 3 （可选）从永远在线 VPN 排除用户。

在 AnyConnect VPN 客户端配置文件中配置永远在线

开始之前

永远在线 VPN 要求在 ASA 上配置有效、受信任的服务器证书；否则它将失败并记录表示证书无效的事件。此外，确保服务器证书能通过严格的证书信任型号可防止永远在线VPN配置文件的下载锁定与欺诈服务器的 VPN 连接。

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **首选项（部分 2）(Preferences [Part 2])**。
步骤 2 选择**自动 VPN 策略 (Automatic VPN Policy)**。
步骤 3 配置值得信赖的网络检测，第 113 页
步骤 4 选择**始终开 (Always On)**。
步骤 5 （可选）选择或取消选择**允许 VPN 断开 (Allow VPN Disconnect)**。
步骤 6 （可选）定义 VPN 在永远在线期间断开连接时，终端可以访问的主机。
步骤 7 （可选）配置连接失败策略。
步骤 8 （可选）配置强制网络门户补救。

向服务器列表添加负载均衡备用集群成员

永远在线 VPN 会影响 AnyConnect VPN 会话的负载均衡。在永远在线 VPN 禁用后，当客户端连接到负载均衡集群中的主设备时，客户端遵守从主设备到任何备用集群成员的重定向。在永远在线 启用后，除非在客户端配置文件的服务器列表中指定备用集群成员的地址，否则客户端不遵守从主设备的重定向。因此，请确保向服务器列表中添加任何备份集群成员。

要在客户端配置文件中指定备用集群成员的地址，请按以下步骤使用 ASDM 添加负载均衡备用服务器列表：

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择**服务器列表 (Server List)**。
步骤 2 选择作为负载均衡集群主设备的服务器，然后单击**编辑 (Edit)**。
步骤 3 输入任何负载均衡集群成员的 FQDN 或 IP 地址。

从永远在线 VPN 排除用户

可以配置豁免以覆盖永远在线策略。例如，您可能要让某些个人建立与其他公司的VPN会话，或者豁免用于非公司资产的永远在线策略。

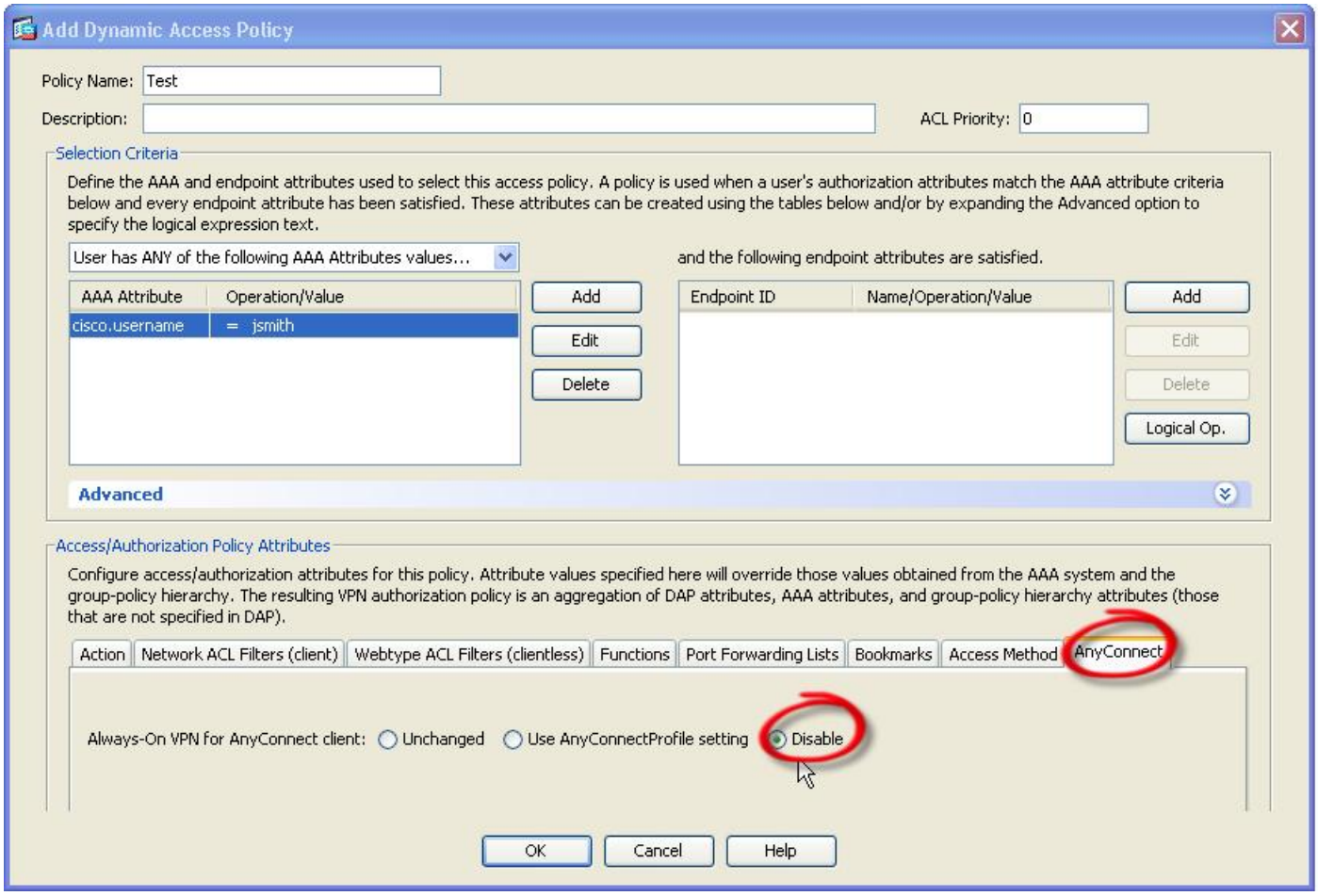
在ASA的组策略和动态访问策略中设置的豁免可覆盖永远在线策略。根据用于分配策略的匹配条件指定例外情况。如果AnyConnect策略启用永远在线，而动态访问策略或组策略禁用它，则只要客户端的条件与建立每个新会话时的动态访问策略或组策略相符，客户端就会对当前和将来的VPN会话保留禁用设置。

此过程配置使用 AAA 终端条件的动态访问策略以将会话匹配至非公司资产。

步骤 1 选择**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **动态访问策略 (Dynamic Access Policies)** > **添加 (Add)** 或**编辑 (Edit)**。

步骤 2 配置条件以豁免来自永远在线 VPN 的用户。例如，使用 Selection Criteria 区域指定匹配用户登录 ID 的 AAA 属性。

步骤 3 单击“添加或编辑动态访问策略”(Add or Edit Dynamic Access Policy) 窗口下半部分的 **AnyConnect** 选项卡。



步骤 4 单击“用于 AnyConnect 客户端的 永远在线 VPN”旁边的**禁用 (Disable)**。

为永远在线设置连接失败策略

关于连接失败策略

如果永远在线 VPN 已启用且 AnyConnect 无法建立 VPN 会话，连接失败策略会确定计算机是否可以访问互联网。当安全网关无法访问，或者 AnyConnect 无法检测到强制网络门户热点的存在时，就会出现这种情况。

开放策略允许完全网络访问，从而使用户可在需要访问互联网或其他本地网络资源时继续执行任务。

封闭策略在 VPN 会话建立前禁用所有网络连接。为此，AnyConnect 启用阻止来自终端（对于允许计算机连接的安全网关不受限制）的所有流量的数据包过滤器。

尽管采用了连接失败策略，AnyConnect 仍会继续尝试建立 VPN 连接。

设置连接失败策略指南

使用允许完全网络访问的开放策略时，请考虑以下内容：

- 直到建立 VPN 会话之后，安全和保护才可用。因此，终端设备可能会受到基于 Web 的恶意软件感染或者泄漏敏感数据。
- 如果启用了“断开”(Disconnect) 按钮且用户单击**断开 (Disconnect)**，则打开连接失败策略不适用。

使用在建立 VPN 会话之前一直禁用所有网络连接的关闭策略时，请考虑以下内容：

- 如果用户需要 VPN 之外的互联网访问，则关闭策略会停止工作。
- 关闭策略旨在当保护终端的专用网络中的资源不可用时帮助保护企业资产免受网络威胁。终端始终受到保护以免遭基于 Web 的恶意软件攻击和防止敏感数据泄漏，因为除分割隧道允许的本地资源（如打印机和外围设备）之外，所有网络访问都被阻止。
- 此选项主要用在网络访问的安全持久性比始终可用性更重要的企业中。
- 关闭策略会阻止强制网络门户补救，除非您专门启用它。
- 如果客户端配置文件中启用了 **Apply Last VPN Local Resources**，则您可以允许应用最新 VPN 会话实施的本地资源规则。例如，这些规则可以确定对活动同步和本地打印的访问权限。
- 若不顾关闭策略而启用了永远在线，则在 AnyConnect 软件升级期间，网络是畅通且开放的。
- 如果您部署关闭连接策略，我们强烈建议您采用分阶段方法。例如，首先利用连接失败打开策略部署永远在线，并向用户调查 AnyConnect 不能无缝连接的频率。然后，在早期采用者用户中部署连接失败关闭策略的一个小型试点部署，并征求他们的反馈。逐步扩展试点计划，同时继续征求反馈，再考虑全面部署。部署连接失败关闭策略时，请确保向 VPN 用户告知网络访问限制以及连接失败关闭策略的优点。

> ⚠ **注意** 如果 AnyConnect 未能建立 VPN 会话，连接故障关闭策略会阻止网络访问。实施连接故障关闭策略时要极度小心谨慎。

配置连接失败策略

仅在永远在线功能启用时才配置连接失败策略。默认情况下，连接失败策略是关闭的，以防止在无法访问 VPN 时访问互联网。要允许在此情况下访问互联网，必须将连接失败策略设置为开放。

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **首选项（部分 2）(Preferences [Part 2])**。

步骤 2 将 **Connect Failure Policy** 参数设置为以下设置之一：

- Closed-（默认值）当无法连接到安全网关时限制网络访问。
- Open - 当客户端无法连接到安全网关时，允许通过浏览器和其他应用访问网络。

步骤 3 如果您指定了关闭策略，请执行以下操作：

a) 配置强制网络门户补救。

b) 如果要在禁用网络访问时保留最后一个 VPN 会话的本地设备规则，请选择 **应用上一个 VPN 本地资源 (Apply Last VPN Local Resources)**。

使用强制网络门户热点检测和补救

关于强制网络门户

许多设施（例如，机场、咖啡店和酒店）提供 Wi-Fi 和有线访问，但可能要求用户在获得访问权之前先付款和/或同意遵守可接受的使用政策。这些设施使用称为强制网络门户的技术来防止应用连接，直到用户打开浏览器并接受访问条件为止。强制网络门户检测用于识别此限制，而强制网络门户补救是满足强制网络门户热点的要求以获取网络访问权限的过程。

在启动无需额外配置的 VPN 连接时，由 AnyConnect 自动检测强制网络门户。此外，AnyConnect 在强制网络门户检测期间不会修改任何浏览器配置设置，且不会自动补救强制网络门户。它依靠最终用户来执行补救。AnyConnect 根据当前配置对强制网络门户检测进行响应：

- 如果永远在线已禁用，或者永远在线已启用且连接失败策略处于打开状态，则在每个连接尝试时显示以下消息：

```
The service provider in your current location is restricting access to the Internet.
You need to log on with the service provider before you can establish a VPN session.
You can try this by visiting any website with your browser.
```

  最终用户必须通过满足热点提供商的要求来执行强制网络门户补救。这些要求可以是付费接入网络、签署可接受使用策略、此两者或提供商规定的一些其他要求。

- 如果永远在线已启用并且连接失败策略关闭，需要明确启用强制网络门户补救。如果已启用，最终用户可以如上文所述执行补救。如果已禁用，则会在每次尝试连接时显示以下消息，且 VPN 无法连接。

```
The service provider in your current location is restricting access to the Internet.
```

```
The AnyConnect protection settings must be lowered for you to log on with the service
provider. Your current enterprise security policy does not allow this.
```

配置强制网络门户补救

仅在永远在线功能启用且连接失败策略设置为关闭时，才配置强制网络门户补救。在这种情况下，可通过配置强制网络门户补救，在强制网络门户阻止 AnyConnect 连接到 VPN 时允许它连接到 VPN。

注释 强制网络门户补救的配置不适用于 Linux，因为此平台不支持无间断。因此，无论配置文件编辑器中的允许强制网络门户补救无间断如何设置，Linux 用户都可以补救强制网络门户。

如果连接失败策略设置为打开或永远在线未启用，则用户对网络的访问不会受到限制，而且用户无需在 AnyConnect VPN 客户端配置文件中进行任何特定配置，即可补救强制网络门户。

在支持无间断的平台（Windows 和 macOS）上，强制网络门户补救默认为禁用以提供最高安全性。在强制网络门户补救阶段，AnyConnect 不提供数据泄漏保护功能。如果需要数据丢失保护，您应使用相关的终端安全产品。

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择**首选项（部分 1）(Preferences [Part 1])**。

步骤 2 选择**允许强制网络门户补救 (Allow Captive Portal Remediation).**

此设置可提升连接失败策略关闭导致的网络访问限制。

步骤 3 指定补救超时。

输入 AnyConnect 提升网络访问限制的分钟数。要满足强制网络门户要求，用户需要足够的时间。

增强的强制网络门户补救（仅限 Windows）

通过增强的强制网络门户补救功能，只要检测到强制网络门户具有受 AnyConnect 限制的网络访问（例如，由于无间断），就会在补救中使用 AnyConnect 嵌入式浏览器。在执行强制网络访问门户时，其他应用仍会受到阻止，同时 AnyConnect 浏览器处于挂起状态。用户可以关闭 AnyConnect 浏览器并故障转移到外部浏览器（如果已在配置文件中启用），这将导致 AnyConnect 复原到常规强制网络门户补救行为。执行此操作时，会显示以下消息：

```
Please retry logging on with the service provider to retain access to the Internet, by
visiting any website with your browser.
```

当检测到强制网络门户而网络访问受 AnyConnect 限制时，系统会自动启动 AnyConnect 浏览器，并显示以下消息提示用户进行补救：

```
The service provider in your current location is restricting access to the internet. You
need to log on with the service provider before you establish a VPN session, using the
AnyConnect browser.
```

配置强制网络门户补救浏览器故障转移

您可能希望将浏览器故障转移设置为每当启动用于强制网络门户补救的AnyConnect浏览器时应用。通过设置浏览器故障转移，用户可以在关闭 AnyConnect 浏览器后通过外部浏览器补救强制网络门户。

为强制网络门户补救启动的AnyConnect浏览器在服务器安全证书方面有着更严格的安全设置。在强制网络门户补救期间，不会接受不受信任的服务器证书。如果遇到不受信任的服务器证书，AnyConnect浏览器不会加载相应的HTTPS URL，这可能会阻止补救过程。如果不受信任的服务器证书在强制网络门户补救期间可接受，则应启用强制网络门户补救浏览器故障转移，以便允许用户对强制网络门户进行补救。启用后，用户可以关闭 AnyConnect 浏览器并继续使用外部浏览器进行补救，（因为 AnyConnect 会复原到常规强制网络门户补救行为）。

开始之前

仅在 Windows 上受支持。

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择**首选项（第 2 部分）(Preferences [Part 2])** 。

步骤 2 如果您希望最终用户使用外部浏览器（在关闭AnyConnect浏览器后）进行强制网络门户补救，请选中**强制网络门户补救浏览器故障转移 (Captive Portal Remediation Browser Failover)**。默认情况下，最终用户仅使用 AnyConnect 浏览器补救强制网络门户；也就是说，用户无法禁用增强的强制网络门户补救。

对强制网络门户检测和补救进行故障排除

AnyConnect 在以下情况下会错误地假设自己处于强制网络门户中。

- 如果 AnyConnect 尝试与包含不正确的服务器名称 (CN) 的证书的 ASA 通信，则 AnyConnect 客户端会认为它处于“强制网络门户”环境中。

  要避免此情况，请确保正确配置了 ASA 证书。证书中的 CN 值必须匹配 VPN 客户端配置文件中 ASA 服务器的名称。

- 如果在 ASA 之前，网络中有另一台设备，且该设备通过阻止对 ASA 的 HTTPS 访问来对客户端尝试联系 ASA 做出响应，则 AnyConnect 客户端会认为它处于“强制网络门户”环境中。当用户位于内部网络且通过防火墙连接 ASA 时，可能发生此情况。

  如果您需要从公司内部限制对 ASA 的访问，请配置防火墙以使至 ASA 地址的 HTTP 和 HTTPS 流量不会返回HTTP状态。应允许或完全阻止对ASA的HTTP/HTTPS访问，以确保发送到ASA的 HTTP/HTTPS 请求不会返回意外响应。

如果用户无法访问强制网络门户补救页面，请要求用户尝试以下操作：

- 终止任何使用 HTTP 的应用，如即时消息程序、邮件客户端、IP 电话客户端和除了一个执行补救的浏览器之外的一切应用。

  强制网络门户可能会通过忽略重复的连接尝试使它们在客户端超时，从而积极地抑制 DoS 攻击。若很多应用都尝试进行 HTTP 连接，会加剧此问题。

- 禁用并重新启用网络接口。此操作会触发强制网络门户检测重试。
- 重启计算机。

通过 L2TP 或 PPTP 配置 AnyConnect

某些国家/地区的 ISP 要求支持第 2 层隧道协议 (L2TP) 和点对点隧道协议 (PPTP)。

要通过点对点协议 (PPP) 连接将流量发送到安全网关，AnyConnect 使用外部隧道生成的点对点适配器。通过 PPP 连接建立 VPN 隧道时，客户端必须从要发送到 ASA 以外目标的隧道流量排除发送目标为 ASA 的流量。要指定是否排除路由及如何确定排除路由，请使用 AnyConnect 配置文件中的 PPP 排除设置。排除路由在 AnyConnect GUI 的 Route Details 中显示为非安全路由。

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **首选项（部分 2）(Preferences [Part 2])**。

步骤 2 选择一种**PPP 排除 (PPP Exclusion)** 方法。此外，为此字段选中**用户可控制 (User Controllable)**，让用户查看和更改此设置：

- Automatic - 启用 PPP 排除。AnyConnect 自动确定 PPP 服务器的 IP 地址。
- 覆盖 (Override) - 使用 *PPP Exclusion Server IP*（*PPP* 排除服务器 *IP*）字段中指定的预定义服务器 IP 地址来启用 PPP 排除。*PPP* 排除服务器 *IP (PPP Exclusion Server IP)* 字段仅适用于此覆盖方法，并且仅在“自动”(Automatic) 选项无法检测 PPP 服务器的 IP 地址时使用。

  为“PPP 排除服务器 IP”(PPP Exclusion Server IP) 选中**用户可控制 (User Controllable)** 字段可允许最终用户通过 preferences.xml 文件手动更新 IP 地址。请参阅 指示用户覆盖 PPP 排除，第 122 页 一节。
- Disabled - 不应用 PPP 排除。

指示用户覆盖 PPP 排除

如果自动检测不起作用，并且您已将 PPP Exclusion 字段配置为用户可控制，则用户可以在本地计算机上通过编辑 AnyConnect 首选文件来覆盖设置。

步骤 1 使用编辑器（如记事本）打开首选 XML 文件。

此文件位于用户计算机上的以下路径之一：

- Windows：%LOCAL_APPDATA%\Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml。例如，
- macOS：/Users/username/.anyconnect
- Linux：/home/username/.anyconnect

步骤 2 在 <ControllablePreferences> 下插入 PPPExclusion 详细信息，同时指定 Override 值和 PPP 服务器的 IP 地址。地址必须是格式正确的 IPv4 地址。例如：

```
<AnyConnectPreferences>
<ControllablePreferences>
<PPPExclusion>Override
<PPPExclusionServerIP>192.168.22.44</PPPExclusionServerIP></PPPExclusion>
</ControllablePreferences>
</AnyConnectPreferences>
```

步骤 3 保存文件。

步骤 4 退出并重新启动 AnyConnect。

使用管理 VPN 隧道

关于管理 VPN 隧道

管理 VPN 隧道可确保客户端系统在开启时连接到企业网络，这不仅限于最终用户建立了 VPN 连接的情况。您可以对办公室外的终端（尤其是用户很少通过VPN连接到办公网络的设备）执行补丁管理。需要企业网络连接的终端操作系统登录脚本也可以得益于此功能。

管理VPN隧道是为了向最终用户提供透明性；因此在默认情况下，用户应用发起的网络流量不会受到影响，而是会被定向到管理 VPN 隧道外部。

当系统检测到已启用管理隧道功能时，系统会创建受限制用户帐户 (ciscoacvpnuser) 以实施最小特权原则。在 AnyConnect 卸载期间或安装升级过程中，此帐户会被删除。

如果用户抱怨登录缓慢，可能表示管理隧道配置不当。配置管理 VPN 隧道，第 125 页描述了启用该功能需要完成的配置步骤。如果症状表明，尽管遵循此配置，但仍然缺乏到企业网络的连接，请参阅管理 VPN 隧道连接问题故障排除。

管理 VPN 隧道的兼容性和要求

- 要求 ASA 9.0.1（或更高版本）和 ASDM 7.10.1（或更高版本）
- 在用户登录之前或之后，每当用户启动的 VPN 隧道断开连接时连接。

注释 当可信网络检测 (TND) 功能检测到可信网络或正在进行 AnyConnect 软件更新时，管理 VPN 隧道未建立。

- 在用户登录之前或之后，每当用户启动 VPN 隧道时，连接断开。
- 仅使用计算机存储证书验证。
- 默认情况下，需要分割包含隧道配置，以免影响用户发起的网络通信（因为管理VPN隧道对最终用户是透明的）。要覆盖此行为，请参阅配置自定义属性以支持全隧道配置 ，第 127 页。

- 对服务器证书执行严格的证书检查。服务器证书根CA证书必须位于计算机证书存储区（Windows上的计算机证书存储区或 macOS 上的系统密钥链或系统文件证书存储区）中。
- 使用备份服务器列表。
- 目前仅在 Windows 和 macOS 上可用。后续版本中会添加对于 Linux 的支持。

管理 VPN 隧道的不兼容性和限制

- 管理 VPN 配置文件不支持将代理设置的值设置为本地。此限制仅适用于 Windows 客户端，因为管理VPN隧道可以在没有任何用户登录的情况下启动；因此，它不能依赖于用户特定的浏览器代理设置。
- 管理 VPN 配置文件不支持从 VPN 服务器推送的专用代理设置。由于管理 VPN 隧道对最终用户是透明的，因此用户特定或系统代理设置不会更改。
- 与“始终打开”功能不兼容，因为只要用户 VPN 隧道处于非活动状态，就会建立管理 VPN 隧道。但是，您可以为管理隧道连接配置组策略以隧道传输所有流量，从而确保在用户VPN隧道处于非活动状态时，物理接口不会泄漏任何流量。请参阅 配置自定义属性以支持全隧道配置，第 127 页。
- 强制网络门户修复仅在 AnyConnect UI 正在运行且用户登录时执行，就像未启用管理 VPN 隧道功能一样。
- 管理 VPN 配置文件设置仅在管理 VPN 隧道处于活动状态时由 AnyConnect 实施。当管理 VPN 隧道断开连接时，仅实施用户 VPN 隧道配置文件设置。因此，管理 VPN 隧道根据用户 VPN 隧道配置文件中值得信赖的网络检测 (TND) 设置启动，即，当 TND 被禁用或检测到“不受信任的网络”时，无论配置的不受信任的网络策略为何。此外，管理 VPN 配置文件中的 TND 连接操作（仅在管理 VPN 隧道处于活动状态时实施）始终适用于用户 VPN 隧道，以确保管理 VPN 隧道对最终用户透明。为获得一致的用户体验，您必须在用户和管理VPN隧道配置文件中使用相同的 TND 设置。

管理 VPN 配置文件强制的必填首选项

在管理VPN隧道处于活动状态时，部分配置文件首选项为必填。为了帮助您配置有效的配置文件，AnyConnect 管理 VPN 配置文件编辑器通过禁用相应的 UI 控件来实施必填首选项。在管理隧道连接期间，以下首选项值会改写，主要是为了消除用户交互并最大限度地减少隧道中断：

- *AllowManualHostInput: false* - 与管理隧道无关（无头客户端）。
- *AlwaysOn: false* - 不相关，因为管理隧道断开连接时，会实施用户隧道配置文件首选项。
- *AutoConnectOnStart: false* - 仅适用于 UI 客户端，用于在启动时自动连接到先前连接的主机。
- *AutomaticCertSelection: true* - 避免证书选择弹出窗口。
- *AutoReconnect: true* - 避免网络更改时管理隧道终止。
- *AutoReconnectBehavior: ReconnectAfterResume* - 避免网络更改时管理隧道终止。
- *AutoUpdate: false* - 管理隧道连接期间不执行任何软件更新。
- *BlockUntrustedServers: true* - 避免不受信任的服务器证书提示。

- *CertificateStore: MachineStore* - 管理隧道验证在没有登录用户的情况下也应该成功。
- *CertificateStoreOverride: true* - Windows 上的计算机证书验证必需。
- *EnableAutomaticServerSelection: false* - 管理 VPN 配置文件中仅应有一个主机项。
- *EnableScripting: false* - 在管理隧道连接期间不会执行 AnyConnect 自定义脚本（在连接和/或断开连接时调用）。
- *MinimizeOnConnect:false* - 与管理隧道无关（无头客户端）。
- *RetainVPNOnLogoff:true* - 管理隧道应在用户注销时保持活动状态。
- *ShowPreConnect Message* - 与管理隧道无关（无头客户端）。
- *UserEnforcement: AnyUser* - 确保在某个用户登录时管理隧道不可能断开连接。
- *UseStartBeforeLogon:False* - 仅适用于用户隧道。
- *WindowsVPNEstablishment: AllowRemote Users* - 确保管理隧道不受任何类型的用户（本地/远程）登录影响。
- *LinuxVPNEstablishment: Allow Remote Users* - 确保管理隧道不受任何类型的用户（本地/远程）影响。

此外，AnyConnect 在管理隧道连接期间不实施以下配置文件首选项：WindowsLogonEnforcement 和 SCEP 相关首选项。

此外，AnyConnect 在管理隧道连接期间不实施以下配置文件首选项：WindowsLogonEnforcement、LinuxLogonEnforcement 和 SCEP 相关首选项。

配置管理 VPN 隧道

由于管理隧道连接可能在没有任何用户登录的情况下发生，因此仅支持计算机存储证书验证。因此，客户端主机的计算机证书存储区中至少需要有一个相关的客户端证书。

为管理 VPN 隧道配置隧道组

您必须在 ASDM 中导航到**配置 (Configuration) > 远程访问 (Remote Access) > 网络（客户端）访问 (Network [Client] Access) > AnyConnect 连接配置文件 (AnyConnect Connection Profiles) > 添加/编辑 (Add/Edit)**，并从“身份验证”(Authentication) 下的“方法”(Method) 下拉菜单中选择“仅证书”(certificate only)，将隧道组的身份验证方法配置为“仅证书”(certificate only)。然后在“高级”>“组别名/组 URL”中配置组 URL（随后会在管理 VPN 配置文件中指定）（如为管理 VPN 隧道创建配置文件，第 126 页中所述）。

此隧道组的组策略必须使用该隧道组中配置的客户端地址分配为所有 IP 协议配置分割包含隧道：从 ASDM **远程访问 VPN (Remote Access VPN) > 网络（客户端）访问 ((Network [Client] Access)) > 组策略 (Group Policies) > 编辑 (Edit) > 高级 (Advanced) > 分割隧道 (Split Tunneling) > 选择下面的隧道网络列表**。配置自定义属性以支持全隧道配置，第 127 页介绍了如何启用对其他分割隧道配置的支持。如果未在隧道组中为两种 IP 协议配置客户端地址分配，则必须在组策略中启用客户端绕行协议，这样管理 VPN 隧道才不会中断与没有客户端地址分配的 IP 协议匹配的流量。

为管理 VPN 隧道创建配置文件

您只能将一个管理 VPN 配置文件部署到给定的客户端设备。管理 VPN 配置文件存储在专用目录（Windows 中是 %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun，macOS 中是 /opt/cisco/anyconnect/profile/mgmttun），有固定名称 (VpnMgmtTunProfile.xml)。管理 VPN 配置文件可以有零个或一个主机条目，指向按照为管理 VPN 隧道配置隧道组，第 125 页部分配置的隧道组。要自动禁用该功能（在隧道建立期间配置文件更新时），应在管理VPN配置文件中配置零个主机条目。

开始之前

完成为管理 VPN 隧道配置隧道组，第 125 页。

步骤 1 导航到 **配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（客户端）访问 (Network [Client] Access) > AnyConnect 客户端配置文件 (AnyConnect Client Profile)**。

步骤 2 单击**添加 (Add)**，“添加 AnyConnect 客户端配置文件”(Add AnyConnect Client Profiles) 窗口即会打开。

步骤 3 选择 **ANYCONNECT 管理 VPN 配置文件**作为要使用的配置文件。有关如何在“添加 AnyConnect 客户端配置文件”屏幕上填充字段的详细说明，请参阅《思科 ASA 系列 VPN ASDM 配置指南》中的“配置 AnyConnect 客户端配置文件”部分。

步骤 4 选择在为管理 VPN 隧道配置隧道组，第 125 页中创建的组策略。单击**确定 (OK)** 创建管理 VPN 配置文件，然后单击**编辑 (Edit)** 以进行配置并完成后续更新。

（可选）上传已配置的管理 VPN 配置文件。

您可能需要将使用独立 AnyConnect 管理 VPN 配置文件编辑器编辑或创建、从 AnyConnect 系统复制或者从其他 ASA 导出的已配置管理 VPN 配置文件上传到ASA。

步骤 1 在 ASDM 的“AnyConnect 客户端配置文件”(AnyConnect Client Profile) 窗口中，依次单击**添加 (Add)** 和**上传...(Upload...)**。。
选择上传文件的目标位置时，请确保选择具有 *vpnm* 扩展名的配置文件。

步骤 2 提供配置文件名称，然后从“要使用的配置文件”(Profile Usage) 下拉菜单中选择 **AnyConnect 管理 VPN 配置文件 (AnyConnect Management VPN Profile)**。

步骤 3 选择在为管理 VPN 隧道配置隧道组，第 125 页中创建的组策略。单击**确定 (OK)** 以创建管理 VPN 配置文件。

将管理 VPN 配置文件关联到组策略

您必须将管理 VPN 配置文件添加到与用于管理隧道连接的隧道组关联的组策略。

注释 同样，也可以将管理VPN配置文件添加到映射至常规隧道组的组策略，用于用户隧道连接。当用户连接时，系统会下载管理 VPN 配置文件以及已映射到组策略的用户 VPN 配置文件，从而启用管理 VPN 隧道功能。

或者，您可以在带外部署管理 VPN 配置文件：确保将其命名为 VpnMgmtTunProfile.xml，将其复制到上文所述的管理 VPN 配置文件目录，然后重新启动思科 AnyConnect 安全移动代理服务（或重新引导）。

开始之前

完成为管理 VPN 隧道配置隧道组，第 125 页和为管理 VPN 隧道创建配置文件，第 126 页。

步骤 1 在 ASDM 中导航到**组策略 (Group Policy) > 高级 (Advanced) > AnyConnect 客户端 (AnyConnect Client)**。

步骤 2 在要下载的客户端配置文件中，单击**添加 (Add)**，然后选择在为管理 VPN 隧道创建配置文件，第 126 页部分创建或更新的管理 VPN 配置文件。

配置自定义属性以支持全隧道配置

默认情况下，管理VPN隧道需要分割包含隧道配置，以免影响用户发起的网络通信（因为管理VPN隧道对最终用户是透明的）。您可以通过在管理隧道连接使用的组策略中配置以下自定义属性来改写此行为（在“创建自定义属性 ASDM”窗口中：**配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略 > 编辑 > 高级 > AnyConnect 客户端 > 自定义属性 > 添加**）。

如果您将新的自定义属性类型设置为 **ManagementTunnelAllAllowed**，并将相应的自定义属性设置为 *true*，则 AnyConnect 将继续进行管理隧道连接，前提是两个 IP 协议都配置为 tunnel-all、split-exclude、split-include 或 bypass 之一。

限制管理 VPN 配置文件更新

您可以使用新的 AnyConnect 本地策略文件 (AnyConnectLocalPolicy.xml) 设置将管理 VPN 配置文件更新限制为某个受信任的服务器列表，并且仍允许来自任何服务器的用户VPN配置文件更新。选中**允许来自任何服务器的 VPN 配置文件更新 (Allow Management VPN Profile Updates From Any Server)** 复选框，通过 本地策略首选项 编辑此设置。

例如，如果仅允许从 VPN 服务器 TrustedServer 进行管理 VPN 配置文件更新，系统会取消选中该复选框，并将 TrustedServer 添加到受信任服务器列表中。（将 TrustedServer 替换为对应 VPN 配置文件服务器条目中的 FQDN 或 IP 地址。）

管理 VPN 隧道连接问题故障排除

如果客户端主机无法远程访问，则可能发生了各种情况，导致管理VPN隧道连接断开或未建立。在这些情况下，AnyConnect VPN GUI 和 CLI 会将管理连接状态反映为统计条目：

- 已断开连接（已禁用）- 功能禁用。

- 已断开连接（受信任的网络）- TND 检测到受信任的网络，因此未建立管理隧道。
- 已断开连接（用户隧道处于活动状态）- 用户隧道当前处于挂起状态（管理隧道因而断开）。
- 已断开连接（进程启动失败）- 尝试管理隧道连接时遇到进程启动故障。
- 已断开连接（连接失败）- 建立管理隧道时遇到连接故障。
- 已断开连接（VPN 配置无效）- 建立管理隧道时遇到无效的分割隧道配置。请参阅配置自定义属性以支持全隧道配置 ，第 127 页获得更多信息。
- 已断开连接（软件更新挂起）- AnyConnect 软件更新当前处于挂起状态（管理隧道因而断开）。
- 已断开连接 - 即将建立或由于其他原因无法建立管理隧道。

要排除管理 VPN 隧道上无连接的问题（预期在客户端主机上建立）, 请验证以下各项：

- 在 CLI 中的“AnyConnect UI 统计信息”(AnyConnect UI Statistics) 选项卡、导出统计信息输出或连接信息/管理连接状态中，检查管理 VPN 连接的状态。如果管理连接状态意外地被列为“断开连接”并且提供的解释不足，请使用 DART 工具捕获 AnyConnect 日志，以便进一步排查故障。
- 如果在 UI 统计信息行中看到管理连接状态：已断开连接（已禁用），请确保管理 VPN 配置文件配置了单个主机条目，指向通过证书身份验证设置的隧道组。关联的组策略必须配置有一个配置文件：管理 VPN 配置文件。

  注释 关联的组策略不应启用横幅。管理隧道连接期间不支持用户交互。

- 如果在 UI 统计信息行中看到管理连接状态：已断开连接（已禁用），请确保在与用于常规用户隧道连接的隧道组关联的组策略中，配置了管理 VPN 配置文件。当用户连接到该隧道组时，系统会下载管理 VPN 配置文件，并启用该功能。

  注释 或者，您也可以在带外部署管理 VPN 配置文件。

- 如果在 UI 统计信息行中看到管理连接状态：已断开连接（连接失败），请注意，当需要用户交互时，管理隧道连接都会出现故障，如下所示：
  - 如果服务器证书不受信任。服务器证书的根 CA 证书必须位于计算机证书存储区中。
  - 如果与计算机存储证书相关的私人密钥受密码保护，则管理隧道连接无法使用对应的客户端证书。客户端证书无法使用，因为系统无法提示用户输入私钥密码。
  - 如果未将 macOS 系统密钥链私钥配置为允许访问而不提示 AnyConnect VPN 代理可执行文件 (vpnagentd)；管理隧道连接无法使用对应的客户端证书，因为系统无法提示用户输入访问私钥的凭证。
  - 如果组策略配置有横幅。

配置 AnyConnect 代理连接

关于 AnyConnect 代理连接

AnyConnect 通过本地、公共和私有代理来支持 VPN 会话：

- 本地代理连接：

  本地代理与 AnyConnect 在同一台计算机上运行，且有时用作透明代理。例如，一些无线数据卡提供的加速软件或一些防病毒软件（例如，Kaspersky）上的网络组件就是透明代理服务。

  本地代理的使用在 AnyConnect VPN 客户端配置文件中启用或禁用，请参阅允许本地代理连接。

- 公共代理连接：

  公共代理通常用于将网络流量匿名化。当 Windows 配置为使用公共代理时，AnyConnect 使用该连接。macOS 和 Linux 也支持使用公共代理作为本地和覆盖选项。

  有关配置公共代理的说明，请参阅公共代理，第 130 页。

- 私有代理连接：

  在企业网络上使用私有代理服务器来基于企业使用政策防止企业用户访问特定网站，例如色情、赌博或游戏站点。

  将组策略配置为在隧道建立后将私有代理设置下载到浏览器。在 VPN 会话结束后，设置恢复到其初始状态。请参阅配置专用代理连接，第 131 页。

注释 通过代理服务器的 AnyConnect SBL 连接取决于 Windows 操作系统版本和系统（机器）配置或其他第三方代理软件功能。因此，请参阅 Microsoft 或您使用的任何第三方代理应用提供的系统范围代理设置。

使用 VPN 客户端配置文件控制客户端代理

VPN 客户端配置文件可以阻止或重定向客户端系统的代理连接。对于 Windows 和 Linux，您可以配置（也可以允许用户配置）公共代理服务器的地址。

有关在 VPN 客户端配置文件中配置代理设置的详细信息，请参阅AnyConnect 配置文件编辑器，首选项（第 2 部分），第 79 页。

生成代理自动配置文件以提供无客户端支持

某些版本的 ASA 需要 AnyConnect 配置才能支持在建立 AnyConnect 会话后通过代理服务器进行无客户端门户访问。为使此情况发生，AnyConnect 使用代理自动配置 (PAC) 文件修改客户端代理设置。仅在 ASA 没有指定私有端代理设置时，AnyConnect 才生成此文件。

AnyConnect 代理连接的要求

代理连接支持的操作系统视情况而定，如下所示：

代理连接类型	Windows 的 ISE 安全评估代理	macOS	Linux
本地代理	是	是（覆盖和本地）	是
私有代理	是（在 Internet Explorer 上）	是（设定为系统代理设置）	否
公共代理	是（IE 和覆盖）	是（覆盖和本地）	是（覆盖和本地）

代理连接的限制

- 当已启用永远在线功能时，不支持通过代理进行连接。
- 要允许访问本地代理，需要一个 VPN 客户端配置文件。

允许本地代理连接

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **首选项（部分 2）(Preferences [Part 2])**。

步骤 2 选择（默认值）或取消选择**允许本地代理连接 (Allow Local Proxy Connections)**。默认情况下本地代理被禁用。

公共代理

公共代理在 Windows 和 Linux 平台上受支持。系统根据在客户端配置文件中设置的首选项选择代理服务器。在代理覆盖的情况下，AnyConnect 从配置文件抽取代理服务器。通过版本 4.1，我们在 macOS 上添加了代理支持，同时还在 Linux 和 macOS 上添加了本地代理配置。

在 Linux 上，在 AnyConnect 运行之前会导出本地代理设置。如果更改设置，则必须重新启动。

向代理服务器进行身份验证需要用户名和密码。当代理服务器配置为需要身份验证时，AnyConnect 支持基本和NTLM身份验证。AnyConnect对话管理身份验证过程。成功向代理服务器进行身份验证后，AnyConnect 会提示输入 ASA 用户名和密码。

配置公共代理连接，Windows

请按照以下步骤在 Windows 上配置公共代理连接。

步骤 1 从 Internet Explorer 或控制面板打开 **Internet Options**。

步骤 2 选择**连接 (Connections)** 选项卡，然后单击 **LAN 设置 (LAN Settings)** 按钮。

步骤 3 配置局域网以使用代理服务器，并输入代理服务器的 IP 地址。

配置公共代理连接，macOS

步骤 1 请转至系统首选项，然后选择您连接的相应接口。

步骤 2 单击**高级 (Advanced)**。

步骤 3 从新窗口中选择**代理 (Proxies)** 选项卡。

步骤 4 启用 HTTPS 代理

步骤 5 在右面板的 Secure Proxy Server 字段中输入代理服务器地址。

配置公共代理连接，Linux

要在 Linux 中配置公共代理连接，您必须设置环境变量。

配置专用代理连接

步骤 1 在ASA组策略中配置私有代理信息。请参阅思科*ASA*系列*VPN*配置指南中的为内部组策略配置浏览器代理部分。

注释 在 macOS 环境中，在打开终端并发出 **`scutil --proxy`** 之前，在浏览器中看不到从 ASA（在 VPN 连接时）向下推送的代理信息。

步骤 2 （可选）将客户端配置为忽略浏览器代理设置。

步骤 3 （可选）锁定 Internet Explorer 的“连接”选项卡。

将客户端配置为忽略浏览器代理设置

您可以在 AnyConnect 配置文件中指定策略以绕过用户 PC 上的 Microsoft Internet Explorer 或 Safari 代理配置设置。这可防止用户在企业网络之外建立隧道，并防止 AnyConnect 通过不需要或非法的代理服务器进行连接。

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **首选项（部分 2）(Preferences [Part 2])**。

步骤 2 在“代理设置”(Proxy Settings) 下拉列表中，选择 **IgnoreProxy**。Ignore Proxy 会使客户端忽略所有的代理设置。不会针对从 ASA 下载的代理执行任何操作。

锁定 Internet Explorer 的“连接”选项卡

在某些情况下，AnyConnect 会隐藏“Internet Explorer 工具 > Internet 选项 > 连接”选项卡。显示此选项卡时，可让用户设置代理信息。隐藏此选项卡可防止用户有意或无意绕过隧道。在连接断开时会撤销选项卡锁定，并且被应用于该选项卡的所有管理员定义的策略所取代。此锁定发生的情况如下：

- ASA 配置指定“连接”选项卡锁定。
- ASA 配置指定私有端代理。
- Windows 组策略之前锁定了“连接”选项卡（覆盖未锁定 ASA 组策略设置）。

您可在组策略中将 ASA 配置为允许或不允许代理锁定。要使用 ASDM 执行此操作，请执行以下操作步骤：

步骤 1 在 ASDM 中，转到**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **组策略 (Group Policies)**。

步骤 2 选择组策略，单击**编辑 (Edit)** 或**添加 (Add)** 可编辑或新增组策略。

步骤 3 在导航窗格中，转到**高级 (Advanced)** > **浏览器代理 (Browser Proxy)**。系统显示 Proxy Server Policy 窗格。

步骤 4 单击**代理锁定 (Proxy Lockdown)** 以显示更多代理设置。

步骤 5 取消选中**继承 (Inherit)** 并选择**是 (Yes)**，可启用代理锁定并在 AnyConnect 会话期间隐藏 Internet Explorer 的“连接”选项卡。或者，选择**否 (No)** 可禁用代理锁定并在 AnyConnect 会话期间显示 Internet Explorer 的“连接”选项卡。

步骤 6 单击**确定 (OK)** 保存代理服务器策略更改。

步骤 7 单击**应用 (Apply)** 保存组策略更改。

验证代理设置

- 对于 Windows：在注册表如下位置找到该代理设置：

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

- 对于 macOS：打开终端窗口，然后输入：

```
scutil --proxy
```

选择并排除 VPN 流量

将 IPv4 或 IPv6 流量配置为绕过 VPN

使用 Client Bypass Protocol 设置，您可以配置 AnyConnect 客户端在 ASA 只需要 IPv6 流量时如何管理 IPv4 流量，或者在 ASA 只需要 IPv4 流量时如何管理 IPv6 流量。

当 AnyConnect 客户端建立与 ASA 的 VPN 连接时，ASA 可以为客户端分配 IPv4 和/或 IPv6 地址。

如果为 IP 协议启用 Client Bypass Protocol，但未对该协议配置地址池（即，未通过 ASA 向客户端分配用于该协议的 IP 地址），则使用该协议的任何 IP 流量都不会通过 VPN 隧道发送，而会在隧道外部发送。

如果禁用 Client Bypass Protocol，且未对该协议配置地址池，则客户端将在 VPN 隧道建立后丢弃该 IP 协议的所有流量。

例如，假设 ASA 只将一个 IPv4 地址分配到 AnyConnect 连接，且终端为双协议栈。当终端尝试连接 IPv6 地址时，如果 Client Bypass Protocol 已禁用，IPv6 流量将被丢弃。如果 Client Bypass Protocol 已启用，IPv6 流量将以明文形式从客户端发送。

如果建立 IPsec 隧道（而不是 SSL 连接），则不会通知 ASA 是否在客户端上启用了 IPv6，因此 ASA 始终推送客户端旁路协议设置。

请在 ASA 的组策略中配置 Client Bypass Protocol。

步骤 1 在 ASDM 中，转到**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **组策略 (Group Policies)**。

步骤 2 选择组策略，单击**编辑 (Edit)** 或**添加 (Add)** 可编辑或新增组策略。

步骤 3 选择**高级 (Advanced)** > **AnyConnect**。

步骤 4 如果该组策略不是默认组策略，请取消选中**客户端绕行协议 (Client Bypass Protocol)** 旁边的**继承 (Inherit)**。

步骤 5 选择以下选项之一：

- 单击**禁用 (Disable)** 以丢弃 ASA 未向其分配地址的 IP 流量。
- 单击**启用 (Enable)** 以明文形式发送该 IP 流量。

步骤 6 单击**确定 (OK)**。

步骤 7 单击**应用 (Apply)**。

配置支持本地打印机和关联设备的客户端防火墙

请参阅思科 *ASA* 系列配置指南中的支持本地打印机和关联设备的客户端防火墙部分。

配置分割隧道

分割隧道在网络（客户端）访问组策略中配置。请参阅思科 ASA 系列 VPN 配置指南中的为 *AnyConnect* 流量配置分割隧道部分。

在 ASDM 中更改组策略后，在 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Group Policy** 中确保组策略与连接配置文件关联。

Linux 上的路由网络流量

要使 Linux 用户能够在 VM 实例/docker 容器上路由网络流量，您必须创建新的自定义属性并启用它。创建 **tunnel-from-any-source** 自定义属性，当设置为 *true* 时，AnyConnect 允许 split-include 或 split-exclude 隧道模式下任何来源地址的数据包，从而允许 VM 实例或 Docker 容器内的网络访问。

注释 VM 实例或 Docker 容器使用的网络最初必须从隧道中排除。

关于动态分割隧道

动态分割隧道旨在增强当前分割隧道选项，这些选项通过 ASDM 组策略配置中的“排除以下网络列表”(Exclude Network List Below) 或“将以下网络列表中的指定网络隧道化”(Tunnel Network List Below) 选项配置。除了通常用于定义分割隧道的静态包含或排除方法外，您还可以使用动态分割隧道包含或排除方法在 VPN 隧道中包含或排除有关特定服务的流量。您无法为每个 IP 协议配置一个不同的分割隧道设置。例如，如果您为 IPv4 启用动态拆分包含隧道（如 IPv4 拆分包含和动态拆分包含域），那么您就无法为 IPv6 启用动态拆分排除隧道（如 IPv6 全隧道和动态拆分排除域）。此外，AnyConnect 4.6 版本还添加了增强的动态分割隧道，其中指定了动态拆分排除和动态拆分包含域以增强域名匹配。

静态分割隧道与动态分割隧道的限制也有所不同。对于静态分割隧道，限制为每个 IP 协议 2500 个网络/ ACE。通过动态分割隧道，AnyConnect 仅考虑具有由前端推送的域列表的前 20,000 个字符的动态分割隧道域，并且仅在客户端上通过截断来实施。不支持使用通配符。

动态拆分排除隧道 - 多个基于云的服务可能托管在同一 IP 池中，并且可能基于用户位置或基于云托管计算资源的负载而解析为不同的 IP 地址。若管理员只想从 VPN 隧道排除单个此类服务，使用静态排除方法定义此类策略就会有些困难（如果还需要考虑 ISP NAT、6to4、4to6 和其他网络转换型号，则更是如此）。通过动态拆分排除隧道，您可以在建立隧道后基于主机 DNS 域名动态调配拆分排除隧道。例如，VPN 管理员可以将 example.com 配置为在运行时从 VPN 隧道中排除。当 VPN 隧道在正常运行且某个应用尝试连接到 mail.example.com 时，VPN 客户端会自动更改系统路由表和过滤器，以允许隧道之外的连接。

增强的动态拆分排除隧道 - 为动态拆分排除隧道配置了动态拆分排除和动态拆分包含域时，从 VPN 隧道动态排除的流量必须至少与一个动态拆分排除域相匹配，但不匹配任何动态拆分包含域。例如，如果 VPN 管理员配置了动态拆分排除域 example.com 和动态拆分包含域 mail.example.com，则除 mail.example.com 以外的所有 example.com 流量都将从隧道中排除。

动态拆分包含隧道 - 通过动态拆分包含隧道，您可以在建立隧道后基于主机 DNS 域名动态调配拆分包含隧道。例如，VPN 管理员可以将 domain.com 配置为在运行时包含在 VPN 隧道中。当 VPN 隧

道在正常运行且某个应用尝试连接到 www.domain.com 时，VPN 客户端会自动更改系统路由表和过滤器，以允许 VPN 隧道内的连接。

增强的动态拆分包含隧道 - 为动态拆分包含隧道配置了动态拆分包含和动态拆分排除域时，动态包含在VPN隧道中的流量必须至少与一个动态拆分包含域相匹配，但不匹配任何动态拆分排除域。例如，如果 VPN 管理员将 domain.com 配置为拆分包含域并将 www.domain.com 配置为拆分排除域，则除 www.domain.com 以外的所有 domain.com 流量都通过隧道传输。

注释 动态分割隧道在 Linux 或任何移动平台中不受支持。

静态分割隧道与动态分割隧道之间的互操作性

静态和动态排除可以共存。静态分割隧道在建立隧道后应用，而动态分割隧道在已连接隧道期间出现传送到域的流量时应用。

动态拆分排除隧道

动态拆分排除隧道应用到“隧道全部”、“拆分包含”和“拆分排除”隧道：

- 隧道全部网络 (Tunnel All Networks) - VPN 隧道中的所有排除都是动态的。
- 排除特定网络 (Exclude Specific Networks) - 动态排除会添加到预配置的静态排除。
- 包含特定网络 (Include Specific Networks) - 仅当已排除主机名至少有一个 IP 地址与拆分包含网络重叠时，动态排除才相关。否则，流量已从 VPN 隧道排除，且不执行任何动态排除。

增强的动态拆分排除隧道适用于“隧道全部”和“拆分排除”隧道。如果配置了动态拆分排除和动态拆分包含域，以及拆分包含隧道，则生成的配置为增强的动态拆分包含隧道。

动态拆分包含隧道

动态拆分包含隧道仅适用于拆分包含配置。

增强的动态拆分包含隧道仅适用于拆分包含配置。

注释 启用静态或动态分割隧道后，Umbrella 漫游安全保护处于活动状态。您可能必须在 VPN 隧道中静态包含或排除 Umbrella 云解析器，除非它们可访问且可由 VPN 隧道探测。

具有分割隧道配置的重叠方案的结果

动态包含或排除仅涵盖尚未包含或排除的 IP 地址。应用了静态和某种形式的动态隧道，且需要强制实施新的动态包含或排除时，可能出现与已应用的包含或排除的冲突。当实施动态排除（包含与已排除的域名匹配且作为 DNS 响应一部分的所有 IP 地址）时，仅考虑排除尚未排除的地址。同样，当强制实施动态包含（包括与已包含的域名匹配且作为 DNS 响应一部分的所有 IP 地址）时，仅考虑包含尚未包含的地址。

静态公共路由（例如安全网关路由等拆分排除和关键路由）优先于动态拆分包括路由。因此，如果动态包含的至少一个 IP 地址与静态公共路由匹配，则不强制实施动态包含。

同样，静态拆分-包含路由优先于动态拆分排除路由。因此，如果动态排除的至少一个 IP 地址与静态拆分（包含路由）匹配，则不强制实施动态排除。

动态分割隧道使用通知

在连接 VPN 隧道后，可以通过以下几种方式查看为动态分割隧道设置的内容：

- “统计”(Statistics) 选项卡 - 显示动态隧道排除和动态隧道包含，其中包括从 VPN 隧道中排除或包含在其中的域名，如 ASA 组策略中所配置的那样。
- Export Stats - 生成一个文件，其中包括从 VPN 隧道中排除或包含在其中的域名，以及用于 IPv4 和 IPv6 的隧道型号。动态路由也包含在导出的统计信息中。
- “路由详细信息”(Route Details) 选项卡 - 显示 IPv4 和 IPv6 动态拆分排除和包含路由，其中包括与每个排除或包含的 IP 地址对应的主机名。

注释 AnyConnect UI 针对每种 IP 协议，最多仅显示 200 条由 AnyConnect VPN 实施的安全或非安全路由。超过 200 条路由时，将会出现截断，并且您可以运行 **route print**（在 Windows 上）或 **netstat-rn** （在 Linux 或 macOS 上）查看所有路由。

- VPN 配置日志消息 - 显示从 VPN 隧道中排除或包含在其中的域数。

配置动态拆分排除隧道

开始之前

请参阅 关于动态分割隧道，第 134 页。

通过动态分割隧道，您可以在建立隧道后基于主机DNS域名动态调配拆分排除隧道。通过创建自定义属性并将其添加到 ASA 上的组策略，可配置动态分割隧道。请参阅《思科 *ASA* 系列 *VPN ASDM* 配置指南》中的配置动态分割隧道，了解 GUI 步骤。

步骤 1 使用以下命令在 WebVPN 上下文中定义自定义属性类型：

```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains
```

步骤 2 定义客户端需要访问的 VPN 隧道外的每个云/Web 服务的自定义属性名称。例如，添加 Google_domains 以表示有关 Google Web 服务的 DNS 域名的列表。属性值包含要从 VPN 隧道中排除且必须为逗号分隔值 (CSV) 格式的域名列表，示例如下：

```
anyconnect-custom-data dynamic-split-exclude-domains example_service_domains example1.com, example2.com
```

步骤 3 使用以下命令将之前定义的自定义属性附加到特定策略组中，该命令在组策略属性上下文中执行：

```
anyconnect-custom dynamic-split-exclude-domains value example_service_domains
```

配置增强的动态拆分排除隧道

开始之前

请参阅 关于动态分割隧道，第 134 页。

当使用动态拆分排除和动态拆分包括域配置了动态拆分排除隧道时，支持增强的域名匹配。通过创建两个自定义属性并将其添加到 ASA 上的组策略，配置增强的动态拆分排除隧道。请参阅《思科 *ASA* 系列 *VPN ASDM* 配置指南》中的配置动态分割隧道，了解 GUI 步骤。

步骤 1 使用以下命令在 WebVPN 上下文中定义自定义属性类型：

```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains
```

步骤 2 定义客户端需要访问的 VPN 隧道外的每个云/Web 服务的自定义属性名称。例如，如果 example.com 是动态拆分排除域，而 www.example.com 是动态拆分包含域，则会排除到 examples.com 的所有流量，www.example.com 除外。属性值包含要从 VPN 隧道中排除（或不排除）且必须为逗号分隔值 (CSV) 格式的域名列表，示例如下：

```
anyconnect-custom-data dynamic-split-exclude-domains example_service_domains example1.com, example2.com
anyconnect-custom-data dynamic-split-include-domains example_service_domains_tunneled www.example1.com,
 www.example2.com
```

步骤 3 使用以下命令将之前定义的自定义属性附加到特定策略组中，该命令在组策略属性上下文中执行：

```
anyconnect-custom dynamic-split-exclude-domains value
example_service_domains
anyconnect-custom dynamic-split-include-domains value
example_service_domains_tunneled
```

配置动态拆分包含隧道

开始之前

请参阅 关于动态分割隧道，第 134 页。

通过动态分割隧道，您可以在建立隧道后基于主机DNS域名动态调配拆分包含隧道。通过创建自定义属性并将其添加到 ASA 上的组策略，可配置动态分割隧道。请参阅《思科 *ASA* 系列 *VPN ASDM* 配置指南》中的配置动态分割隧道，了解 GUI 步骤。

步骤 1 使用以下命令在 WebVPN 上下文中定义自定义属性类型：

```
anyconnect-custom-attr dynamic-split-include-domains description dynamic split include domains
```

步骤 2 定义需要通过 VPN 隧道进行客户端访问的每个云/Web 服务的自定义属性名称。属性值包含要包含在 VPN 隧道中且必须为逗号分隔值 (CSV) 格式的域名列表，示例如下：

```
anyconnect-custom-data dynamic-split-include-domains corporate_service_domains domain1.com, domain2.com
```

注释 自定义属性不能超过 421 个字符。如果超出限制，动态包含域（以 CSV 格式）的列表可能需要分成较小的值。

步骤 3 使用以下命令将之前定义的自定义属性附加到特定策略组中，该命令在组策略属性上下文中执行：

```
anyconnect-custom dynamic-split-include-domains value
corporate_service_domains
```

配置增强的动态拆分包含隧道

开始之前

请参阅 关于动态分割隧道，第 134 页。

当使用动态拆分包含和动态拆分排除域配置了动态拆分包含隧道时，支持增强的域名匹配。通过创建两个自定义属性并将其添加到 ASA 上的组策略，配置增强的动态拆分包含隧道。请参阅《思科 *ASA* 系列 *VPN ASDM* 配置指南》中的配置动态分割隧道，了解 GUI 步骤。

步骤 1 使用以下命令在 WebVPN 上下文中定义自定义属性类型：

```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains
```

步骤 2 定义需要通过 VPN 隧道进行客户端访问的每个云/Web 服务的自定义属性名称。例如，当 domain.com 是动态拆分包含域，而 www.domain.com 是动态拆分排除域时，将包含到 domain.com 的所有流量，www.domain.com 除外。属性值包含要包含（或不包含）在 VPN 隧道中且必须为逗号分隔值 (CSV) 格式的域名列表，示例如下：

```
anyconnect-custom-data dynamic-split-include-domains corporate_service_domains domain1.com, domain2.com
anyconnect-custom-data dynamic-split-include-domains corporate_service_domains_excluded www.domain1.com,
 www.domain2.com
```

步骤 3 使用以下命令将之前定义的自定义属性附加到特定策略组中，该命令在组策略属性上下文中执行：

```
anyconnect-custom dynamic-split-include-domains value
corporate_service_domains
anyconnect-custom dynamic-split-exclude-domains value
corporate_service_domains_excluded
```

拆分 DNS

拆分包含和拆分排除隧道配置均支持拆分 DNS。

在网络（客户端）访问策略中为拆分包括隧道配置拆分 DNS 时，AnyConnect 将通过隧道向 VPN DNS 服务器传送指定 DNS 查询（同时也在组策略内配置）。所有其他 DNS 查询都会定向到 VPN 隧道之外并传送至公共 DNS 服务器。

在为拆分排除隧道配置拆分 DNS 时，指定 DNS 查询将在 VPN 隧道外部发送到公共 DNS 服务器。所有其他 DNS 查询均通过隧道传输到 VPN DNS 服务器。

如果未配置拆分 DNS，AnyConnect 将通过隧道传送所有 DNS 查询。

拆分 DNS 的要求

Windows 和 macOS 平台均支持拆分 DNS。

- Linux 上仅提供有限的支持，即仅隧道 DNS 请求须受拆分 DNS 策略的限制。因此，隧道外部发送的某些 DNS 请求可能不符合拆分 DNS 策略。

对于 macOS，仅当满足以下条件之一时，AnyConnect 才能对特定 IP 协议使用真拆分 DNS：

- 为组策略中的一种 IP 协议（例如 IPv4）配置分割 DNS 并为另一种 IP 协议（例如 IPv6）配置客户端绕行协议（对后一种 IP 协议不配置地址池）。
- 为两个 IP 协议都配置分离 DNS。

如果为一个 IP 协议配置了用于拆分包含的拆分 DNS，并且为另一个协议配置了拆分排除的拆分 DNS，则拆分包含的拆分 DNS 的优先级更高，从而导致 AnyConnect 忽略拆分排除拆分的 DNS 设置。

拆分 DNS 仅与依赖本地/操作系统 DNS 客户端进行名称解析的典型应用程序相关，例如浏览器、邮件应用程序等。不支持的应用程序包括使用自定义解析器的工具，例如 dig 和 nslookup。

为拆分包括隧道配置拆分 DNS

要在组策略中为拆分包括隧道配置拆分 DNS，请执行以下操作：

步骤 1 配置至少一个 DNS 服务器。

请参阅思科 ASA 系列 VPN 配置指南中的为内部组策略配置服务器属性部分。

确保指定的专用 DNS 服务器与客户端平台配置的 DNS 服务器不重叠。如果重叠，则域名解析可能无法正常工作。

步骤 2 配置拆分 - 包含隧道：

在**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络 (客户端) 访问 (Network (Client) Access) > 组策略 (Group Policies) > 高级 (Advanced) > 分割隧道 (Split Tunneling)**窗格中，选择**隧道化以下网络列表 (Tunnel Network List Below)** 策略，然后指定要隧道化的地址的**网络列表 (Network List)**。

步骤 3 在**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络 (客户端) 访问 (Network (Client) Access) > 组策略 (Group Policies) > 高级 (Advanced) > 分割隧道 (Split Tunneling)** 窗格中，取消选中**通过隧道发送所有 DNS 查找 (DNS lookups through tunnel)**，然后在 **DNS 名称 (DNS Names)** 中指定其查询需要隧道化的域的名称。

下一步做什么

在 ASDM 中更改组策略后，在 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Group Policy** 中确保组策略与连接配置文件关联。

为拆分排除隧道配置拆分 DNS

要在组策略中为拆分排除隧道配置拆分 DNS，请执行以下操作：

步骤 1 在 ASDM 中，导航到 **Configuration**（配置）> **Remote Access VPN**（远程访问 VPN）> **Network (Client) Access**（网络[客户端]访问）> **Advanced**（高级）> **AnyConnect Custom Attributes**（**AnyConnect 定制属性**）以配置新的定制属性类型。选择**添加 (Add)** 并在“创建定制属性”(Create Custom Attribute) 窗格中设置以下项：

a) 输入 **split-dns-exclude-domains** 作为新的类型。
b) 或者，输入说明。

步骤 2 要为创建的类型配置新的自定义属性名称，请选择**添加 (Add)** 并在创建自定义属性名称窗格中设置以下内容：

a) 为类型选择 **split-dns-exclude-domains**。
b) 输入名称。
c) 对于该值，输入其查询不应通过隧道传输的域名的列表，域名以逗号分隔。
客户端最多接受 300 个此类域。不支持使用通配符。

步骤 3 选择**添加 (Add)** 并在“创建定制属性”(Create Custom Attribute) 窗格中设置以下项：

a) 为“属性类型”(Attribute Type) 字段选择在步骤 1 中创建的类型。
b) 为“值”(Value) 字段选择在第 2 步中创建的名称。

步骤 4 至少配置一个 VPN DNS 服务器。

请参阅思科 ASA 系列 VPN 配置指南中的为内部组策略配置服务器属性部分。

确保指定的专用DNS服务器与客户端平台配置的DNS服务器不重叠。如果重叠，则域名解析可能无法正常工作。

步骤 5 配置拆分排除或动态拆分排除隧道。

在 **配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（客户端）访问 (Network [Client] Access) > 组策略 (Group Policies) > 高级 (Advanced) > 分割隧道 (Split Tunneling)** 窗格中，选择**排除以下网络列表 (Exclude Network List Below)** 策略，然后指定要排除的地址的网络列表。

有关其他信息，请参阅配置动态拆分排除隧道 ， 第 136 页。不支持具有拆分包含隧道的动态拆分排除配置。

步骤 6 在 **配置 (Configuration) > 远程访问 VPN (Remote Access VPN)> 网络（客户端）访问 (Network [Client] Access)> 组策略 (Group Policies) > 高级 (Advanced) > 分割隧道 (Split Tunneling)** 窗格中，取消选中**通过隧道发送所有 DNS 查找 (Send All DNS lookups through tunnel)**。

下一步做什么

在 ASDM 中更改组策略后，在 **Configuration**（配置）> **Remote Access VPN**（远程访问 VPN）> **Network (Client) Access**（网络[客户端]访问）> **AnyConnect Connection Profiles**（**AnyConnect 连接配置文件**）> **Add/Edit**（添加/编辑）> **Group Policy**（组策略）中确保组策略与连接配置文件关联。

使用 AnyConnect 日志验证拆分 DNS

要验证是否启用了拆分 DNS，请搜索 AnyConnect 日志中包含“Received VPN Session Configuration Settings”的条目。IPv4 拆分 DNS 和 IPv6 拆分 DNS 有各自的日志条目。

- 对于拆分 DNS，排除：
  - IPv4 拆分 DNS：5 个排除的域
  - IPv6 拆分 DNS：5 个排除的域
- 对于拆分 DNS，包括：
  - IPv4 拆分 DNS：包含 5 个域
  - IPv6 拆分 DNS：包含 5 个域

管理 VPN 身份验证

重要安全注意事项

我们不建议在您的安全网关上使用自签证书

- 因为用户可能会在无意中将浏览器配置为信任欺诈服务器上的证书，并且
- 用户在连接到安全网关时还有必须响应安全警告的不便。

我们强烈建议您为 AnyConnect 客户端启用严格证书信任。要配置 **Strict Certificate Trust**（**严格证书信任**），请参阅本地策略参数和值一节：本地策略首选项，第 100 页。

支持的安全类型

AnyConnect 支持将 RSA 和 ECDSA 证书用于服务器证书验证和客户端证书身份验证。

- **RSA 证书**

  AnyConnect 支持具有以下属性的 RSA 证书：

  - 密钥长度 2048、4096 或 8192 位
  - 散列算法 MD5*、SHA1、SHA256、SHA384 或 SHA512

    *AnyConnect 在 FIPS 模式下运行时，不支持使用 MD5 散列的 RSA 证书。

- **ECDSA 证书**

  AnyConnect 支持具有以下属性的 ECDSA 证书：

  - 密钥长度为 256、384 或 521 位。这些长度分别对应于 NIST P-256、P-384 和 P-521 椭圆曲线。

- **EdDSA 证书**

  AnyConnect 依赖 Windows 和 macOS 操作系统来建立信任并通过数字证书来执行签名操作。由于这些操作系统还不支持 EdDSA 证书，因此 AnyConnect 也无法支持它们。

配置服务器证书处理

服务器证书验证

- 证书必须满足上述最小密钥大小，并且是支持类型之一（RSA 或 ECDSA）。
- （仅限 Windows）对于 SSL 和 IPsec VPN 连接，可以选择执行证书吊销列表 (CRL) 检查。在配置文件编辑器中启用此设置后，AnyConnect将检索链中所有证书的已更新CRL。随后它将验证有关证书是否包含在不应再受信任的这些已吊销证书中；如果发现该证书已被证书颁发机构 (CA) 吊销，则不进行连接。有关详细信息，请参阅本地策略首选项，第 100 页。
- 当用户连接到使用服务器证书配置的ASA时，系统仍将显示表示信任并导入该证书的复选框，即便信任链（根证书、中间证书等）存在问题也是如此。如果存在其他证书问题，则不显示该复选框。
- 如果使用 FQDN 的初始验证失败，则通过 FQDN 执行的 SSL 连接不会进行第二次服务器证书验证（包括使用 FQDN 的解析 IP 地址进行名称验证）。
- 执行验证的日期和时间（由操作系统报告）必须在证书的有效期开始日期之后和有效期结束日期之前。
- 服务器证书不需要密钥使用 (KU) 或扩展密钥使用 (EKU) 获得接受，但不建议此做法。但是，如果存在这些字段（最常见），则适用以下条件：

  对于 SSL 和 IPsec（RSA 和 ECDSA 证书），任何 KU 字段都必须包含 DigitalSignature。对于 RSA 证书，KU 还必须包含 KeyEncipherment 或 KeyAgreement。

  对于 IPsec VPN，任何 EKU 字段都必须包含 ServerAuth 或 IkeIntermediate。
- IPsec 和 SSL 连接将对服务器证书执行名称验证。以下规则适用于 IPsec 和 SSL 名称验证：
  - 如果存在具有相关属性的主题备选名称扩展，则仅对主题备选名称执行名称验证。相关属性包括针对所有证书的 DNS 名称属性，此外，如果针对某一 IP 地址执行连接，则还包括 IP 地址属性。
  - 如果不存在主题备选名称扩展，或存在主题备选名称扩展但不包含相关属性，则对证书主题中找到的任何公用名称属性执行名称验证。
  - 如果证书出于名称验证目的而使用了通配符，则通配符只能位于第一个（最左）子域，且必须是子域中的最后一个（最右）字符。出于名称验证的目的而将忽略任何不合规的通配符条目。
- 对于 OSX，过期的证书仅在密钥链访问配置为 Show Expired Certificates 时显示。默认情况下，过期的证书将隐藏，这可能会给用户造成困扰。

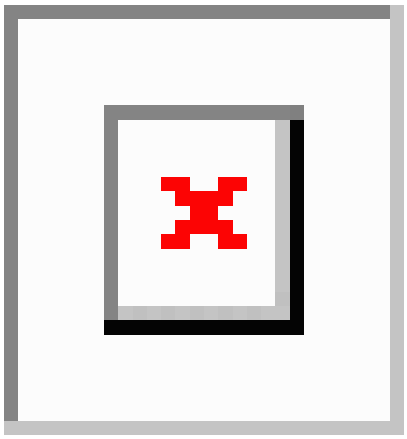
无效的服务器证书处理

为了应对不断增加的针对不受信任网络上移动用户的定向攻击，我们改进了客户端的安全保护，以帮助阻止严重的安全漏洞。默认的客户端行为已更改，以提供一层额外防御来阻挡中间人攻击。

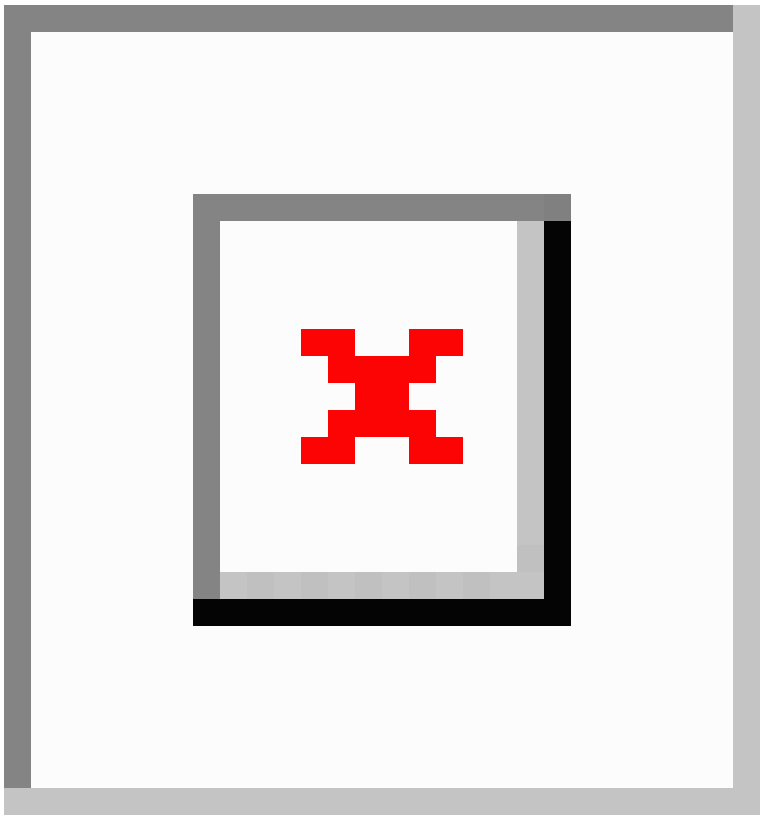
用户交互

当用户尝试连接到安全网关，并且存在证书错误（由于过期、日期无效、密钥使用错误或 CN 不匹配）时，用户会看到一个红色对话框，其中含有 Change Settings 和 Keep Me Safe 按钮。

注释 Linux 下的对话框可能看起来与本文档所示的对话框不同。



- 单击**保障我的安全 (Keep Me Safe)** 将取消连接。
- 单击**更改设置 (Change Settings)** 将打开 AnyConnect 的“高级”(Advanced) > VPN > “首选项”(Preferences) 对话框，用户可在其中启用与不受信任服务器的连接。当前连接尝试将被取消。



如果用户取消选中**阻止与不受信任的服务器的连接 (Block connections to untrusted servers)**，并且唯一的证书问题是 CA 不受信任，则用户下次尝试连接到此安全网关时，将看不到“证书阻止错误”(Certificate Blocked Error Dialog) 对话框；他们只会看到以下对话框：

如果用户选中**始终信任此 VPN 服务器并导入证书 (Always trust this VPN server and import the certificate)** 选项，则未来与此安全网关的连接不会提示用户继续。

注释 如果用户在 **AnyConnect 高级 (AnyConnect Advanced) > VPN > 首选项 (Preferences)** 中选中**阻止连接到不受信任的服务器 (Block connections to untrusted servers)**，或者如果用户的配置满足准则和限制一节所述模式列表中的条件之一，则不管是否在“配置文件编辑器”(Profile Editor) 中启用了“严格证书信任”(Strict Certificate Trust) 选项，AnyConnect 都将拒绝无效的服务器证书和不受信任的服务器连接。

改进的安全行为

当客户端接受无效的服务器证书时，该证书保存在客户端的证书存储库中。以前，仅保存证书的拇指指纹验证。请注意，仅当用户选择始终信任并导入无效服务器证书时，才保存无效证书。

不会出现管理权限改写而自动导致最终用户安全性降低的情况。要完全删除最终用户先前的安全决策，请在用户的本地策略文件中启用 **Strict Certificate Trust**。启用 Strict Certificate Trust 后，用户将看到一条错误消息，并且连接失败；没有用户提示。

有关在本地策略文件中启用 Strict Certificate Trust 的信息，请参阅本地策略首选项，第 100 页中的 *AnyConnect* 本地策略参数和值部分。

指南和限制

在以下情况下将拒绝无效服务器证书：

- AnyConnect VPN 客户端配置文件启用了 Always on，并且应用的组策略或 DAP 未将其关闭。
- 客户端的本地策略启用了 Strict Certificate Trust。
- AnyConnect 配置为在登录前启动。
- 使用机器证书存储库中的客户端证书进行身份验证。

配置仅证书身份验证

您可以指定想要用户使用 AAA 通过用户名和密码进行身份验证，还是使用数字证书验证（或同时使用两种方式）。配置仅证书身份验证时，用户可以使用数字证书进行连接，不需要提供用户 ID 和密码。

为了在使用多个组的环境中支持仅通过证书身份验证，您可以配置多个组 URL。每个组 URL 包含一个不同的客户端配置文件，其中包含一些定制数据，以允许创建特定于组的证书映射。例如，可在 ASA 上调配工程部的 Department_OU 值，以便在此过程中的证书显示给 ASA 时将用户放入此组。

注释 用于向安全网关验证客户端身份的证书必须有效且受信任（由 CA 签署）。不接受自签客户端证书。

步骤 1 转到**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network (Client) Access)** > **AnyConnect 连接配置文件 (AnyConnect Connection Profiles)**。选择一个连接配置文件，然后单击“编辑”(Edit)。系统将打开 Edit AnyConnect Connection Profile 窗口。

步骤 2 单击窗口左侧窗格中导航树的**基本 (Basic)** 节点（如果尚未单击）。在窗口右窗格的 **Authentication** 区域中，启用 **Certificate** 方法。

步骤 3 单击**确定 (OK)** 应用更改。

配置证书注册

Cisco AnyConnect Secure Mobility Client 使用简单证书注册协议 (SCEP) 在客户端身份验证过程中调配和续订证书。采用以下方式通过 AnyConnect IPsec 和 SSL VPN 连接到 ASA 来支持使用 SCEP 的证书注册：

- SCEP 代理：ASA 作为客户端与证书颁发机构 (CA) 之间 SCEP 请求和响应的代理。
  - CA 必须能够接入 ASA，而不是 AnyConnect 客户端，因为客户端不会直接访问 CA。
  - 注册始终会由客户端自动发起。无需用户参与。

相关主题

AnyConnect 配置文件编辑器，证书注册 ，第 87 页

SCEP 代理注册和操作

以下步骤说明如何获取证书，以及在为 SCEP 代理配置 AnyConnect 和 ASA 时如何建立基于证书的连接。

1. 用户使用为证书和 AAA 身份验证配置的连接配置文件连接到 ASA 前端。ASA 向客户端请求证书和 AAA 凭证进行身份验证。
2. 用户输入其 AAA 凭证，但有效证书不可用。此情形将在使用输入的 AAA 凭证建立隧道之后触发客户端发送一个自动 SCEP 注册请求。
3. ASA 将注册请求转发到 CA，并将 CA 的响应返回客户端。
4. 如果 SCEP 注册成功，则客户端向用户显示一条（可配置的）消息，并断开当前会话连接。现在，用户即可使用证书身份验证连接到 ASA 隧道组。

   如果SCEP注册失败，客户端会向用户显示一条（可配置）消息并断开当前会话连接。用户应与其管理员联系。

其他 SCEP 代理操作注意事项：

- 如果进行了相应的配置，则客户端将在证书过期之前自动续订，无需用户干预。
- SCEP 代理注册使用 SSL 进行 SSL 和 IPsec 隧道证书身份验证。

证书颁发机构要求

- 支持所有符合 SCEP 的 CA，包括 IOS CS、Windows Server 2003 CA 和 Windows Server 2008 CA。
- CA 必须处于自动授予型号。不支持证书轮询。
- 您可以将某些CA配置为将注册密码用邮件发送给用户，以增加一层安全保护。CA 密码是发送到证书颁发机构来识别用户的质询密码或令牌。然后，密码被配置在AnyConnect客户端配置文件中，此配置文件成为授予证书之前 CA 验证的 SCEP 请求的一部分。

证书注册指南

- 对 ASA 的无客户端（基于浏览器的）VPN 访问不支持 SCEP 代理，但 WebLaunch（无客户端发起的 AnyConnect）支持 SCEP 代理。
- ASA 负载均衡支持通过 SCEP 注册。
- ASA 并不指出注册失败的原因，尽管它记录从客户端收到的请求。必须在 CA 或客户端上调试连接问题。
- ASA 上的仅通过证书身份验证和证书映射：

  为了在使用多个组的环境中支持仅通过证书身份验证，您可以配置多个组 URL。每个组 URL 包含一个不同的客户端配置文件，其中包含一些定制数据，以允许创建特定于组的证书映射。例如，会在 ASA 上配置 Engineering 的 Department_OU 值，以便当来自此进程的证书呈现给 ASA 时将用户放入此隧道组中。
- 识别注册连接应用策略。

  在 ASA 上，aaa.cisco.sceprequired 属性可用于捕获注册连接和在选择的 DAP 记录中应用适当的策略。
- Windows 证书警告：

  Windows 客户端在首次尝试从证书颁发机构获得证书时可能收到一条警告。出现提示时，用户必须单击“是”(Yes)。这会允许他们导入根证书。它不影响他们使用客户端证书进行连接。

配置 SCEP 代理证书注册

为 SCEP 代理注册配置 VPN 客户端配置文件

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择**认证登记 (Certificate Enrollment)**。

步骤 2 选择**认证登记 (Certificate Enrollment)**。

步骤 3 配置在注册证书中要请求的 **Certificate Contents**。有关证书字段的定义，请参阅 AnyConnect 配置文件编辑器，证书注册。

注释
- 如果您使用 %machineid%，则必须为桌面客户端加载 HostScan/Posture。
- 对于移动客户端，必须指定至少一个证书字段。

配置 ASA 以支持 SCEP 代理注册

对于 SCEP 代理，一个 ASA 连接配置文件支持证书注册和证书的授权 VPN 连接。

步骤 1 创建组策略，例如，cert_group。设置以下字段：
- 在 General 中的 **SCEP Forwarding URL** 内输入 CA 的 URL。
- 在“高级”(Advanced) > “AnyConnect 客户端”(AnyConnect Client) 窗格中，取消选中要下载的客户端配置文件的**继承 (Inherit)**，并指定为 SCEP 代理配置的客户端配置文件。例如，指定 ac_vpn_scep_proxy 客户端配置文件。

步骤 2 为证书注册和证书授权连接创建连接配置文件，例如 cert_tunnel。
- 身份验证：两者（AAA 和证书）。
- 默认组策略：cert_group。
- 在“高级”(Advanced) > “常规”(General) 中，选中**启用此连接配置文件的 SCEP 注册 (Enable SCEP Enrollment for this Connction Profile)**。
- 在 Advanced > GroupAlias/Group URL 中，创建包含此连接配置文件的组 (cert_group) 的组 URL。

为 SCEP 设置 Windows 2008 服务器证书颁发机构

如果证书颁发机构软件在 Windows 2008 服务器上运行，您可能需要对服务器做出以下配置更改之一，以支持 SCEP 与 AnyConnect 一起使用。

在证书颁发机构上禁用 SCEP 密码

以下步骤说明如何禁用 SCEP 质询密码，以便客户端无需在 SCEP 注册之前提供带外密码。

步骤 1 在认证中心服务器上，启动注册编辑器。您可以通过依次选择**开始 (Start)** > **运行 (Run)**，键入 **regedit** 并单击**确定 (OK)** 来执行此操作。

步骤 2 导航到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword。

如果 EnforcePassword 密钥不存在，请将其创建为新密钥。

步骤 3 编辑 EnforcePassword，并将其设置为“0”。如果不存在，请将其创建为 REG-DWORD。

步骤 4 退出 regedit，然后重新引导证书颁发机构服务器。

在证书颁发机构上设置 SCEP 模板

以下步骤说明如何创建证书模板，并将其指定为默认的 SCEP 模板。

步骤 1 启动 Server Manager。可通过选择“开始”(Start)>“管理工具”(Admin Tools)>“服务器管理器”(Server Manager) 执行此操作。

步骤 2 展开 Roles > Certificate Services（或 AD Certificate Services）。

步骤 3 导航到 CA Name > Certificate Templates。

步骤 4 右键单击**证书模板 (Certificate Templates) > 管理 (Manage)**。

步骤 5 从“证书模板控制台”(Cert Templates Console) 中，右键单击用户模板并选择**复制 (Duplicate)**

步骤 6 为新模板选择 **Windows Server 2008 version**，然后单击**确定 (OK)**。

步骤 7 将模板显示名更改为描述性名称，如 NDES-IPSec-SSL。

步骤 8 调整站点的有效期。大多数站点选择三年或更长有效期以避免证书过期。

步骤 9 在“密码”(Cryptography) 选项卡中，为部署设置最小密钥长度。

步骤 10 在“主题名称”(Subject Name) 选项卡中，选择**应要求提供 (Supply in Request)**。

步骤 11 在“扩展”(Extensions) 选项卡中，将“应用程序策略”(Application Policies) 设置为至少包括：

- 客户端身份验证
- IP 安全端系统
- IP 安全 IKE intermediate
- IP 安全隧道终止
- IP 安全用户

这些值对于 SSL 或 IPsec 有效。

步骤 12 单击**应用 (Apply)**，然后单击**确定 (OK)** 保存新模板。

步骤 13 从“服务器管理器”(Server manager) >“证书服务-CA 名称”(Certificate Services-CA Name)，右键单击“证书模板”(Certificate Templates)。选择“新建”(New) >“要颁发的证书模板”(Certificate Template to Issue)，然后选择您创建的新模板（在本示例中为 NDES-IPSec-SSL）并单击**确定 (OK)**。

步骤 14 编辑注册表。您可以通过选择“开始”(Start) >“运行”(Run)、regedit 并单击**确定 (OK)** 执行此操作。

步骤 15 导航到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP。

步骤 16 将以下三个关键字的值设置为 **NDES-IPSec-SSL**。

- EncryptionTemplate
- GeneralPurposeTemplate
- SignatureTemplate

步骤 17 单击**保存 (Save)**，并重新启动证书颁发机构服务器。

配置证书到期通知

配置 AnyConnect 以提醒用户其身份验证证书即将到期。**Certificate Expiration Threshold** 设置指定 AnyConnect 在证书到期之前多少天提醒用户其证书即将到期。AnyConnect 在每次连接时都会提醒用户，直到证书实际到期或已获取新证书。

注释 证书到期阈值功能不能与 RADIUS 一起使用。

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择**认证登记 (Certificate Enrollment)**。

步骤 2 选择**认证登记 (Certificate Enrollment)**。

步骤 3 指定 **Certificate Expiration Threshold**。

这是 AnyConnect 在证书到期前提醒用户其证书即将到期的天数。

默认值为 0（不显示警告）。范围为 0 至 180 天。

步骤 4 单击**确定 (OK)**。

配置证书选择

以下步骤显示 AnyConnect 配置文件中可以配置证书搜索方式的所有位置，以及在客户端系统中选择证书的方式。这些都不是必须执行的步骤，如果您未指定任何条件，AnyConnect 将使用默认密钥匹配。

AnyConnect 读取 Windows 上的浏览器证书存储区。对于 Linux，必须创建隐私增强邮件 (PEM) 格式的文件存储。对于 macOS，可以使用隐私增强邮件 (PEM) 格式的文件存储或密钥链。

步骤 1 Windows 和 macOS：配置要使用的证书存储区，第 151 页

在 VPN 客户端配置文件中指定 AnyConnect 使用的证书存储库。

步骤 2 仅限 Windows：提示 Windows 用户选择身份验证证书，第 153 页

配置 AnyConnect，为用户显示有效的证书列表，让他们选择证书以对会话进行身份验证。

步骤 3 对于 macOS 和 Linux 环境：为 macOS 和 Linux 创建 PEM 证书存储区，第 154 页

步骤 4 对于 macOS 和 Linux 环境：在 VPN 本地策略配置文件中选择要排除的证书存储库。

步骤 5 配置证书匹配，第 154 页

配置 AnyConnect 在存储库中搜索证书时尝试匹配的密钥。您可以指定密钥、扩展密钥，并添加定制扩展密钥。还可以使用可分辨名称指定 AnyConnect 匹配的运算符值型号。

配置要使用的证书存储区

对于 Windows、macOS 和 Linux，系统会为 VPN 客户端配置文件中使用的 AnyConnect 提供单独的证书存储库。您可以有一种或多种证书身份验证组合并可配置安全网关，以指令客户端对于特定的 VPN 连接，可以接受多种证书身份验证选项中的哪一种。例如，在 macOS 上，如果您在本地策略文件中将 ExcludePemFileCertStore 设置为 *true*（以强制 AnyConnect 仅使用本地密钥链证书存储库），并将基于配置文件的证书存储库设置为“登录”（以强制 AnyConnect 仅使用证书存储库，例如用户登录和动态智能卡密钥链，以及用户 PEM 文件存储区），则 AnyConnect 中的组合过滤结果将严格使用用户登录密钥链证书存储库。

对于 Windows，拥有计算机管理权限的用户有权访问两个证书存储库。没有管理权限的用户只能访问用户证书存储库。通常，Windows 用户不具备管理权限。选择**Windows 证书存储库覆盖 (Windows Certificate Store Override)** 将允许 AnyConnect 访问计算机存储库，即使在用户没有管理权限时也是如此。

注释 计算机存储库的访问控制会因 Windows 版本和安全设置而异。因此，即使用户具备管理权限，也可能无法使用计算机存储库中的证书。在此情况下，选择**证书存储库覆盖 (Certificate Store Override)** 可允许访问计算机存储库。

下表描述 AnyConnect 如何基于搜索何种**证书存储区 (Certificate Store)** 以及是否选中 **Windows 证书证书存储区覆盖 (Windows Certificate Store Override)** 从而在客户端中搜索证书。

Certificate Store 设置	**Certificate Store Override 设置**	**AnyConnect 搜索策略**
所有（对于 Windows）	false	AnyConnect 搜索所有的证书存储库。当用户不具备管理权限时，不允许 AnyConnect 访问计算机存储库。 该设置为默认设置。此设置适合大多数情况。请勿更改此设置，除非有特定原因或场景要求这样做。
所有（对于 Windows）	true	AnyConnect 搜索所有的证书存储库。当用户不具备管理权限时，允许 AnyConnect 访问计算机存储库。

Certificate Store 设置	Certificate Store Override 设置	AnyConnect 搜索策略
计算机（对于 Windows）	true	AnyConnect 仅搜索计算机证书存储库。当用户不具备管理权限时，允许 AnyConnect 访问计算机存储库。
所有（对于 macOS）	不适用	AnyConnect 使用所有可用 macOS 密钥链和文件存储区的证书。
用户（对于 Windows）	不适用	AnyConnect 只在用户证书存储库中进行搜索。证书存储库覆盖不适用，原因是没有管理权限的用户可以访问此证书存储库。
系统（对于 macOS）	不适用	AnyConnect 仅使用 macOS 系统密钥链和系统文件/PEM 存储区的证书。仅使用 macOS 系统密钥链和系统文件/PEM 存储区的证书。
登录（对于 macOS）	不适用	AnyConnect 仅使用 macOS 登录和动态智能卡密钥链以及用户文件/PEM 存储区的证书。
全部（对于 Linux）	不适用	AnyConnect 使用系统和用户 PEM 文件存储区以及用户 Firefox NSS 存储区的客户端证书。
计算机（对于 Linux）	不适用	AnyConnect 仅使用系统 PEM 文件存储区中的客户端证书存储库。
用户（对于 Linux）	不适用	AnyConnect 仅使用来自用户 PEM 文件存储区以及用户 Firefox NSS 存储区的客户端证书。

使用多重证书身份验证

开始之前

- 仅在桌面平台（Windows、macOS 和 Linux）上受支持。
- 您必须已在 VPN 配置文件中启用了 *AutomaticCertSelection*。

- 您在该 VPN 配置文件中设置的证书匹配配置将限制可用于多重证书身份验证的证书。

注释 不支持 SCEP。

步骤 1 设置 **Certificate Store**：

- 对于一个计算机证书和一个用户证书，请在 VPN 配置文件中设置为 **All**（**全部**），并按适用于 Windows 的步骤 2 中所述启用 *CertficateStoreOverride*。
- 对于两个用户证书，请在 VPN 配置文件中设置为 **All**（**全部**）或 **User/Login**（**用户/登录**），但按适用于 Windows 的步骤 2 中所述保留 *CertificateStoreOverride*。

步骤 2 如果要在用户不具备管理权限时允许AnyConnect搜索计算机证书存储区，请选择**Windows证书存储库覆盖 (Windows Certificate Store Override)**。

使用基本证书身份验证

步骤 1 设置 **Certificate Store**（**证书存储区**）。

- All - 指示 AnyConnect 客户端使用所有证书存储库来定位证书。
- Machine/System（计算机/系统）— 指示 AnyConnect 客户端仅在本地计算机/系统级别证书存储库中查找证书。
- User/Login（用户/登录）— 指示 AnyConnect 客户端仅在本地用户证书存储库中查找证书。

步骤 2 如果要在用户不具备管理权限时允许AnyConnect搜索计算机证书存储区，请选择**Windows证书存储库覆盖 (Windows Certificate Store Override)**。

提示 Windows 用户选择身份验证证书

您可以将AnyConnect配置为向用户显示有效证书列表并让他们选择证书以对会话进行身份验证。已到期的证书未必会视作无效。例如，如果使用的是SCEP，则服务器可能会向客户端颁发新证书。消除已到期的证书可能会完全阻止客户端进行连接，因此需要手动干预和频带外证书分发。AnyConnect仅限制基于与安全相关的属性（例如密钥用途、密钥类型和强度等）的客户端证书，具体取决于配置的证书匹配规则。此配置仅对 Windows 可用。默认情况下，用户证书选择被禁用。

步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **首选项**（**部分 2**）**(Preferences [Part 2])**。

步骤 2 要启用证书选择，请取消选中**禁用证书选择 (Disable Certificate Selection)**。

步骤 3 取消选中**用户可控制 (User Controllable)**，除非您要用户能够在**高级 (Advanced)** > **VPN** > **首选项 (Preferences)**窗格中打开和关闭自动证书选择。

为 macOS 和 Linux 创建 PEM 证书存储区

AnyConnect 支持从隐私增强型邮件 (PEM) 格式化文件存储区中检索证书。AnyConnect 从远程计算机上的文件系统读取 PEM 格式化的证书文件，对其进行验证和签署。

开始之前

为了使客户端在任何情况下都能获得适当的证书，请确保您的文件满足以下要求：

- 所有证书文件必须以扩展名 .pem 或 .crt 结尾。
- 所有的私钥文件都必须以扩展名 .key 结尾。
- 客户端证书及其对应的私有密钥必须具有相同的文件名。例如：client.pem 和 client.key。

提示 可以使用指向 PEM 文件的软链接，而不是保留 PEM 文件的副本。

要创建PEM文件证书存储区，请创建如下列出的路径和文件夹。将相应的证书置于这些文件夹中：

PEM 文件证书存储区文件夹	所存储证书的类型
~/.cisco/certificates/ca 注释 .cisco/ 位于主目录中。	受信任 CA 和根证书
~/.cisco/certificates/client	客户端证书
~/.cisco/certificates/client/private	私有密钥

计算机证书与 PEM 文件证书相同（除了根目录）。对于计算机证书，用 /opt/.cisco 替代 ~/.cisco。否则，将应用列出的证书的路径、文件夹和类型。AnyConnect 还使用系统 CA 证书位置 (/etc/ssl/certs) 验证服务器证书。

配置证书匹配

AnyConnect 可将其证书搜索限于匹配一组特定密钥的证书。证书匹配是在 AnyConnect VPN 客户端配置文件的**证书匹配**窗格中设置的全局条件。条件包括：

- 密钥使用
- 扩展密钥使用
- 可分辨名称

相关主题

AnyConnect 配置文件编辑器，证书匹配，第 84 页

配置密钥使用

选择**密钥用途 (Key Usage)** 密钥会将 AnyConnect 可用的证书限于至少有一个所选密钥的证书。支持的密钥列在 VPN 客户端配置文件的 **Key Usage** 列表中，其中包括：

- DECIPHER_ONLY
- ENCIPHER_ONLY
- CRL_SIGN
- KEY_CERT_SIGN
- KEY_AGREEMENT
- DATA_ENCIPHERMENT
- KEY_ENCIPHERMENT
- NON_REPUDIATION
- DIGITAL_SIGNATURE

如果指定一个或多个条件，证书必须匹配至少一个条件才被视为匹配的证书。

配置扩展密钥使用

选择**扩展密钥用途 (Extended Key Usage)** 密钥会将 AnyConnect 可用的证书限于具有这些密钥的证书。下表列出一组已知的限制条件及其对应的对象标识符 (OID)。

限制条件	OID
serverAuth	1.3.6.1.5.5.7.3.1
ClientAuth	1.3.6.1.5.5.7.3.2
CodeSign	1.3.6.1.5.5.7.3.3
EmailProtect	1.3.6.1.5.5.7.3.4
IPSecEndSystem	1.3.6.1.5.5.7.3.5
IPSecTunnel	1.3.6.1.5.5.7.3.6
IPSecUser	1.3.6.1.5.5.7.3.7
TimeStamp	1.3.6.1.5.5.7.3.8
OCSPSign	1.3.6.1.5.5.7.3.9
DVCS	1.3.6.1.5.5.7.3.10
IKE Intermediate	1.3.6.1.5.5.8.2.2

配置自定义扩展匹配密钥

所有其他 OID（例如本文档的一些示例中所使用的 1.3.6.1.5.5.7.3.11）被视为“自定义”。作为管理员，如果您所需的 OID 未包含在众所周知的集合中，则可以添加自己的 OID。

配置证书可分辨名称

Distinguished Name 表包含证书标识符，用于将客户端可以使用的证书限于符合指定条件的证书。单击**添加 (Add)** 按钮以在列表中添加条件，并且设置值或通配符以与添加了条件的内容匹配。

标识符	描述
CN	SubjectCommonName
SN	SubjectSurName
GN	SubjectGivenName
N	SubjectUnstructName
I	SubjectInitials
GENQ	SubjectGenQualifier
DNQ	SubjectDnQualifier
C	SubjectCountry
L	SubjectCity
SP	SubjectState
ST	SubjectState
O	SubjectCompany
OU	SubjectDept
T	SubjectTitle
EA	SubjectEmailAddr
DC	DomainComponent
ISSUER-CN	IssuerCommonName
ISSUER-SN	IssuerSurName
ISSUER-GN	IssuerGivenName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier

标识符	描述
ISSUER-DNQ	IssuerDnQualifier
ISSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr
ISSUER-DC	IssuerDomainComponent

Distinguished Name 可以包含零个或多个匹配条件。证书必须匹配所有指定的条件才被视为匹配的证书。**Distinguished Name** 匹配指定证书必须或不能具有指定的字符串，并且指定是否允许对字符串使用通配符。

使用 SAML 进行 VPN 身份验证

可以使用与 ASA 版本 9.7.1 集成的 SAML 2.0 进行初始会话身份验证。AnyConnect 4.6 引入了一个增强版的与嵌入浏览器的 SAML 集成，以替换以前版本中的本机（外部）浏览器集成。当连接到为 SAML 身份验证配置的隧道组时，AnyConnect 会打开一个嵌入式浏览器窗口以完成身份验证过程。每次SAML尝试都使用新的浏览器会话，而浏览器会话特定于AnyConnect（会话状态不与任何其他浏览器共享）。尽管每次 SAML 身份验证尝试在开始时都没有会话状态，但尝试之间仍保持永久 cookie。

平台特定的要求

您必须满足以下系统要求，才能在嵌入式浏览器中使用 SAML：

- Windows - Windows 7（和更高版本）、Internet Explorer 11（和更高版本）
- macOS - macOS 10.10（或更高版本）（AnyConnect 正式支持 macOS 10.11 或更高版本）
- Linux - WebKitGTK+ 2.1 x（或更高版本）、Red Hat 7.4（或更高版本）官方软件包和 Ubuntu 16.04（或更高版本）

升级过程

具有本机（外部）浏览器的 SAML 2.0 在 AnyConnect 4.4 和 AnyConnect 4.5 以及 ASA 9.7.x、9.8.x 和 9.9.1 版中可用。具有嵌入式浏览器的全新增强版本要求升级到 AnyConnect 4.6（或更高版本）和 ASA 9.7.1.24（或更高版本）、9.8.2.28（或更高版本）或 9.9.2.1（或更高版本）。

在升级或部署具有嵌入式浏览器 SAML 集成的前端或客户端设备时，请注意以下情况：

- 如果您先部署 *AnyConnect 4.6*，则本机（外部）浏览器和嵌入式浏览器 SAML 集成将按预期进行，无需进一步操作。AnyConnect 4.6 支持现有的或已更新的 ASA 版本，即使首先部署 AnyConnect 也是如此。
- 如果您首先部署更新的 *ASA* 版本（具有嵌入式浏览器 *SAML* 集成），则必须依次升级 AnyConnect，因为默认情况下，更新的 ASA 版本与 AnyConnect 4.6 之前版本的本机（外部）浏览器 SAML 集成不向后兼容。任何现有 AnyConnect 4.4 或 4.5 客户端的升级都在身份验证之后进行，并且要求您在隧道组配置中启用 **saml external-browser** 命令。

在使用 SAML 时，请遵循以下指导原则：

- 如果在故障转移型号下使用永远在线 VPN，则不支持外部 SAML IdP（但是，使用内部 SAML IdP，ASA 会代理到 IdP 的所有流量并且受支持）
- 在嵌入式浏览器中不允许不受信任的服务器证书。
- CLI 或 SBL 型号中不支持嵌入式浏览器 SAML 集成。
- （仅移动设备）不支持单一注销。
- 在网络浏览器中建立的 SAML 身份验证不会与 AnyConnect 共享，反之亦然。
- 根据具体配置，在使用嵌入式浏览器连接到前端时，会使用各种不同的方法。例如，尽管 AnyConnect 相比于 IPv6 连接更喜欢 IPv4 连接，但嵌入式浏览器可能更喜欢 IPv6，或反之亦然。同样，在尝试代理和收到失败后，AnyConnect 可能会回退到没有代理状态，而嵌入式浏览器在尝试代理并收到失败后可能会停止导航。
- 为了使用 SAML 功能，必须使您的 ASA 网络时间协议 (NTP) 服务器与 IdP NTP 服务器同步。
- ASDM 上的 VPN 向导目前不支持 SAML 配置。
- SAML IdP *NameID* 属性确定用户的用户名，并且用于授权、记帐和 VPN 会话数据库。
- 如果您希望用户每次通过 SAML 建立 VPN 会话时，都使用身份提供程序 (IdP) 重新进行身份验证，则应该在 AnyConnect 配置文件编辑器，首选项（第 1 部分），第 74 页中将 Auto Reconnect 设置为 *ReconnectAfterResume*。
- 由于具有嵌入式浏览器的 AnyConnect 会针对每个 VPN 尝试使用新的浏览器会话，因此，如果 IdP 使用 HTTP 会话 cookie 来跟踪登录状态，则用户每次都必须重新进行身份验证。这种情况下，**配置 > 远程接入 VPN > 无客户端 SSL VPN 接入 > 高级 > 单点登录服务器** > 中的强制重新验证设置对 AnyConnect 启动的 SAML 身份验证没有任何影响。

有关其他配置详细信息，请参阅相应版本（9.7 或更高版本）的思科 ASA 系列 VPN 配置指南中的使用 *SAML 2.0* 的 *SSO* 部分。

使用 SDI 令牌 (SoftID) 集成进行 VPN 身份验证

AnyConnect 支持在 Windows 7 x86（32 位）和 x64（64 位）上运行 RSA SecurID 客户端软件 1.1 版和更高版本。

RSA SecurID 软件验证器可减少用户为确保企业资产访问安全而需要管理的项目数量。远程设备上的 RSA SecurID 软件令牌将生成一个随机的一次性验证码，该验证码每 60 秒变更一次。术语 SDI 的全称是 Security Dynamics, Inc. 技术，指代这一项使用硬件和软件令牌的一次性密码生成技术。

通常情况下，用户通过单击工具托盘中的 AnyConnect 图标、选择希望连接的连接配置文件，然后在身份验证对话框中输入适当的凭证来建立 AnyConnect 连接。登录（质询）对话框将匹配为用户所属的隧道组配置的身份验证类型。登录对话框中的输入字段可明确表明身份验证需要哪类输入。

对于 SDI 身份验证，远程用户需要在 AnyConnect 软件界面中输入 PIN（个人识别码）并接收 RSA SecurID 验证码。用户在安全应用中输入验证码后，RSA 身份验证管理器将验证该验证码并准许用户获得访问权限。

使用 RSA SecurID 硬件或软件令牌的用户将看到输入字段，这些字段指示用户应输入验证码或 PIN，PIN 或验证码以及对话框底部的状态行可提供更多要求信息。用户直接向 AnyConnect 用户界面输入软件令牌 PIN 或密码。

初始登录对话框的外观取决于安全网关设置：用户可通过主登录页面、主索引 URL、隧道组登录页面或隧道组 URL（URL/隧道组）访问安全网关。要通过主登录页面访问安全网关，则必须在“网络(客户端)访问 AnyConnect 连接配置文件 (Network (Client) Access AnyConnect Connection Profiles)”页面上选中“允许用户选择连接 (Allow user to select connection)”复选框。在任何一种情况中，安全网关都会向客户端发送登录页面。主登录页面具有可供用户选择隧道组的下拉列表。由于在 URL 中指定隧道组，隧道组登录页面不含下拉列表。

在主登录页面（具有连接配置文件或隧道组的下拉列表）上，默认隧道组的身份验证类型将确定密码输入字段标签的初始设置。例如，如果默认隧道组使用 SDI 身份验证，则字段标签为“Passcode”，但如果默认隧道组使用 NTLM 身份验证，字段标签为“Password”。在 2.1 版及更高版本中，字段标签不会因用户选择不同的隧道组而动态更新。对于隧道组登录页面，字段标签将与隧道组要求匹配。

客户端支持在密码输入字段中输入 RSA SecurID 软件令牌 PIN。如果安装 RSA SecurID 软件令牌软件，并且隧道组身份验证类型为 SDI，则字段标签为“Passcode”，并且状态栏会声明“Enter a username and passcode or software token PIN”。如果使用 PIN，则针对同一隧道组和用户名的后续连续登录都将包含“PIN”字段标签。客户端使用输入的 PIN 从 RSA SecurID 软件令牌 DLL 检索验证码。每次身份验证成功后，客户端均会保存隧道组、用户名以及身份验证类型，保存的隧道组将成为新的默认隧道组。

AnyConnect 接受针对任意 SDI 身份验证的验证码。即使密码输入标签为“PIN”，用户仍可按照状态栏的指示输入验证码。客户端将按照原样向安全网关发送验证码。如果使用验证码，则针对同一隧道组和用户名的后续连续登录都将包含“Passcode”字段标签。

RSASecureIDIntegration 配置文件设置有三个可能的值：

- Automatic - 客户端首先尝试一种方法，如果失败，则尝试另一种方法。默认将用户输入视为令牌验证码 (HardwareToken)，如果失败，则将其视为软件令牌 PIN (SoftwareToken)。如果身份验证成功，该成功方法将设置为新 SDI 令牌类型，并缓存在用户首选项文件中。对于下一次身份验证尝试，SDI 令牌类型将定义首先尝试的方法。通常，用于当前身份验证尝试的令牌与上次成功身份验证尝试中使用的令牌相同。然而，当用户名或组选择更改时，它将恢复为首先尝试默认方法，如输入字段标签所示。

注释 SDI 令牌类型仅在自动设置中有意义。当身份验证型号不是自动型号时，可以忽略 SKI 令牌类型的日志。HardwareToken 作为默认选项可避免触发下一个令牌型号。

- SoftwareToken - 客户端始终将用户输入视为软件令牌 PIN，输入字段标签为“PIN:”。
- HardwareToken - 客户端始终将用户输入视为令牌验证码，输入字段标签为“Passcode:”。

注释 AnyConnect 不支持将多个令牌的令牌选择导入 RSA 软件令牌客户端软件。相反，客户端使用通过 RSA SecurID 软件令牌 GUI 选择的默认选项。

SDI 身份验证交换的类别

所有 SDI 身份验证交换均属于以下类别之一：

- 普通 SDI 身份验证登录
- 新用户型号
- 新 PIN 型号
- 清除 PIN 型号
- 下一个令牌码型号

普通 SDI 身份验证登录

普通登录质询始终用作第一个质询。SDI 身份验证用户必须分别在用户名和验证码或 PIN 字段中提供用户名和令牌验证码（或者在使用软件令牌时提供 PIN）。客户端将信息返回到安全网关（中心站点设备），然后安全网关使用身份验证服务器（SDI 或通过 RADIUS 代理的 SDI）对身份验证进行验证。

如果身份验证服务器接受身份验证请求，则安全网关会将成功页面发送回客户端，身份验证交换完成。

如果验证码不被接受，则身份验证失败，安全网关会发送一个新的登录质询页面以及一条错误消息。如果达到 SDI 服务器上的验证码失败次数阈值，则 SDI 服务器会将令牌放入下一个令牌码型号中。

新用户型号、清除 PIN 型号和新 PIN 型号

PIN 只能在 SDI 服务器上由网络管理员清除。

在新用户型号、清除 PIN 型号和新 PIN 型号中，AnyConnect 缓存用户创建的 PIN 或系统分配的 PIN，供以后在“下一个验证码”登录质询中使用。

从远程用户的角度来看，清除 PIN 型号和新用户型号是相同的，而且安全网关对两者同等对待。在这两种情况下，远程用户要么必须输入新 PIN，要么由 SDI 服务器分配一个新 PIN。唯一的区别在于对初始质询的用户响应。

对于新 PIN 型号，现有 PIN 用于生成验证码，就像在任何普通质询中一样。对于清除 PIN 型号，硬件令牌根本不会使用 PIN，用户只需输入令牌码。连续八个零 (00000000) 的 PIN 用于为 RSA 软件令牌生成验证码。无论哪种情况，SDI 服务器管理员都必须通知用户使用什么 PIN 值（如果有的话）。

将新用户添加到 SDI 服务器与清除现有用户的 PIN 这两种操作会得到相同的结果。在这两种情况下，用户必须提供新 PIN 或者由 SDI 服务器分配一个新 PIN。在这些型号中，对于硬件令牌，用户只需从 RSA 设备输入一个令牌码。无论哪种情况，SDI 服务器管理员都必须通知用户使用什么 PIN 值（如果有的话）。

创建新 PIN

如果没有当前 PIN，则 SDI 服务器要求满足以下条件之一（具体取决于系统的配置）：

- 系统必须给用户分配一个新 PIN（默认值）
- 用户必须创建一个新 PIN
- 用户可以选择创建 PIN 或由系统分配 PIN

如果 SDI 服务器配置为允许远程用户选择是创建 PIN 还是由系统分配 PIN，则登录屏幕会显示一个包含这些选项的下拉列表。状态行提供提示消息。

对于系统分配的 PIN，如果 SDI 服务器接受用户在登录页面上输入的验证码，则安全网关会向客户端发送系统分配的 PIN。客户端向安全网关发送回响应，表示用户看到了新 PIN，系统继续“下一个验证码”质询。

如果用户选择创建新 PIN，则 AnyConnect 会显示一个对话框以便输入该 PIN。PIN 必须是一个 4 到 8 位的数字。由于 PIN 是一种类型的密码，用户在这些输入字段中输入的任何内容都显示为星号。

使用 RADIUS 代理时，PIN 确认是继原始对话框之后的一个单独质询。客户端将新 PIN 发送到安全网关，安全网关继续“下一个验证码”质询。

“下一个验证码”和“下一个令牌代码”质询

对于“下一个验证码”质询，客户端使用在创建或分配新 PIN 过程中缓存的 PIN 值从 RSA SecurID 软件令牌 DLL 检索下一个验证码并将其返回给安全网关，而不会提示用户。同样，对于软件令牌的“下一个令牌代码”质询，客户端从 RSA SecurID 软件令牌 DLL 检索下一个令牌代码。

比较本地 SDI 与 RADIUS SDI

网络管理员可以配置安全网关，以允许通过以下型号之一进行 SDI 身份验证：

- 本地 SDI 指安全网关中与 SDI 服务器直接通信以便处理 SDI 身份验证的本地能力。
- RADIUS SDI 指安全网关使用 RADIUS SDI 代理（与 SDI 服务器通信）执行 SDI 身份验证的过程。

对于远程用户而言，本地 SDI 和 RADIUS SDI 看起来是相同的。由于 SDI 消息在 SDI 服务器上可配置，ASA 上的消息文本必须与 SDI 服务器上的消息文本匹配。否则，向远程客户端用户显示的提示可能不适合身份验证过程中所需的操作。AnyConnect 可能无法响应，并且身份验证可能失败。

RADIUS SDI 质询基本上反映本地 SDI 交换，仅有极少例外情况。因为两者最终都与 SDI 服务器进行通信，需从客户端获取的信息和索取信息的顺序相同。

在身份验证过程中，RADIUS 服务器向 ASA 显示访问质询消息。这些质询消息中有包含来自 SDI 服务器的文本的应答消息。ASA 直接与某 SDI 服务器通信时的消息文本与通过 RADIUS 代理通信时的消息文本不同。因此，为了向 AnyConnect 显示为本地 SDI 服务器，ASA 必须解析来自 RADIUS 服务器的消息。

此外，由于 SDI 消息在 SDI 服务器上可配置，ASA 的消息文本必须与 SDI 服务器的消息文本（全部或部分）匹配。否则，向远程客户端用户显示的提示可能不适用于身份验证期间所需的操作。AnyConnect 可能无法响应，并且身份验证可能失败。

配置 ASA 以支持 RADIUS/SDI 消息

要配置 ASA 以解释特定于 SDI 的 RADIUS 回复消息并提示 AnyConnect 用户执行相应的操作，您必须配置连接配置文件（隧道组），以模拟与 SDI 服务器直接通信的方式转发 RADIUS 回复消息。用户对 SDI 服务器进行身份验证时，必须通过此连接配置文件进行连接。

步骤 1 转到**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network (Client) Access)** > **AnyConnect 连接配置文件 (AnyConnect Connection Profiles)**。

步骤 2 选择要配置来解释特定于 SDI 的 RADIUS 回复消息的连接配置文件，然后单击**编辑 (Edit)**。

步骤 3 在**编辑 AnyConnect 连接配置文件 (Edit AnyConnect Connection Profile)** 窗口中，展开左侧导航窗格中的“高级”(Advanced) 节点，然后选择 **组别名/组 URL (Group Alias/Group URL)**。

步骤 4 选中**启用登录屏幕上的 SecurID 消息显示 (Enable the display of SecurID messages on the login screen)**。

步骤 5 单击**确定 (OK)**。

步骤 6 依次选择**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **AAA/本地用户 (AAA/Local Users)** > **AAA 服务器组 (AAA Server Groups)**。

步骤 7 单击**添加 (Add)** 以添加 AAA 服务器组。

步骤 8 在“编辑 AAA 服务器组”(Edit AAA Server Group) 对话框中配置 AAA 服务器组，然后单击**确定 (OK)**。

步骤 9 在 **AAA 服务器组 (AAA Server Groups)** 区域，选择您刚刚创建的 AAA 服务器组，然后单击**选定组中的服务器 (Servers in the Selected Group)** 区域中的**添加 (Add)**。

步骤 10 在 SDI 消息区域中，展开 **Message Table** 区域。双击消息文本字段以编辑消息。在 ASA 上配置 RADIUS 回复消息文本以匹配（全部或部分）RADIUS 服务器发送的消息文本。

下表显示消息代码、默认 RADIUS 回复消息文本和每个消息的功能：

注释 ASA 使用的默认消息文本是思科安全访问控制服务器 (ACS) 使用的默认消息文本。如果您使用思科安全 ACS，且它使用默认消息文本，则您无需在 ASA 上配置消息文本。

由于安全设备按字符串在表中显示的顺序搜索字符串，因此您必须确保用于消息文本的字符串不是另一字符串的子集。例如，对于 new-pin-sup 和 next-ccode-and-reauth，“new PIN”均是默认消息文本的一部分。如果您将 new-pin-sup 配置为“new PIN”，则当安全设备从 RADIUS 服务器收到“new PIN with the next card code”时，它将此文本与 new-pin-sup 代码（而不是 next-ccode-and-reauth 代码）匹配。

消息代码	默认 RADIUS 应答消息文本	功能
next-code	Enter Next PASSCODE	表示用户必须输入不含 PIN 的 NEXT 令牌代码。
new-pin-sup	Please remember your new PIN	表示已提供新的系统 PIN 并向用户显示该 PIN。
new-pin-meth	Do you want to enter your own pin	来自用户的请求，表明要使用哪种新的 PIN 方法创建新的 PIN。
new-pin-req	Enter your new Alpha-Numerical PIN	表示用户生成的 PIN 并请求用户输入此 PIN。
new-pin-reenter	Reenter PIN:	在内部由 ASA 用于确认用户提供的 PIN。客户端确认 PIN 而不提示用户。
new-pin-sys-ok	New PIN Accepted	表示已接受用户提供的 PIN。
next-ccode-and-reauth	new PIN with the next card code	遵循 PIN 操作，表示用户必须等待下一个令牌代码并输入新 PIN 和下一个令牌代码才能进行身份验证。
ready-for-sys- pin	ACCEPT A SYSTEM GENERATED PIN	在内部由 ASA 用于表示用户已为系统生成的 PIN 做好准备。

步骤 11 单击**确定 (OK)**，然后单击**应用 (Apply)**，再单击**保存 (Save)**。

关于证书锁定

AnyConnect 证书锁定有助于检测服务器证书链是否确实来自连接服务器。此功能根据 VPN 配置文件设置运行，是 AnyConnect 服务器证书验证策略的附加功能。AnyConnect 本地策略文件中的严格证书信任设置不会对证书锁定检查产生任何影响。您可以在VPN配置文件中全局配置锁定，或按主机配置锁定。针对主要主机配置的锁定也将对服务器列表中的备用主机有效。用户无法更改证书锁定检查的首选项。锁定验证失败会导致 VPN 连接终止。

注释 只有在已启用首选项且 VPN 配置文件中包含与连接服务器相关的锁定设置时，AnyConnect 才会执行锁定验证。

在 VPN 配置文件编辑器 AnyConnect 配置文件编辑器，证书锁定，第 89 页中，您可以启用首选项并配置全局证书锁定和按主机的证书锁定。

在配置和维护证书锁定时，必须保持谨慎。当设置首选项时，请考虑以下建议：

- 锁定根证书和/或中间证书，因为这些证书在操作系统中得到了 CA 供应商的良好维护
- 锁定多个来自不同 CA 的根证书和/或中间证书，以便在任何 CA 受到影响时作为备用证书
- 锁定多个根证书和/或中间证书，以简化 CA 过渡
- 如果锁定某个枝叶证书，请使用相同的证书签名请求在证书续期时保留公共密钥
- 锁定服务器列表中的所有连接主机

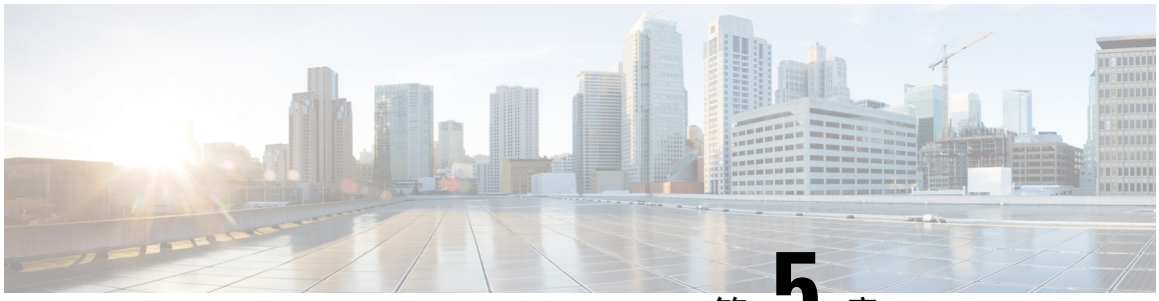
全局和每主机锁定

您可以全局或按主机配置证书锁定。对于大多数连接主机有效的锁定会配置为全局锁定。我们建议您在VPN配置文件中的全局锁定下配置根、中间证书颁发机构和通配符叶证书。仅对连接主机有效的锁定被视为按主机锁定。我们建议在 VPN 配置文件中的按主机锁定下配置自签名叶证书。

注释 AnyConnect 会在锁定验证过程中检查对应的连接服务器的全局锁定和按主机锁定。

注释 多个 VPN 配置文件中的全局锁定不会合并。用于 VPN 连接的文件连接服务器会严格审视锁定。

注释 仅当在全局锁定部分中启用了证书锁定首选项时，才可锁定按主机证书。



第 5 章

配置网络访问管理器

本章提供网络访问管理器的配置概述以及添加和配置用户策略和网络配置文件的说明。

关于网络访问管理器

网络访问管理器是依据其策略提供安全第 2 层网络的客户端软件。可检测并选择最佳第 2 层接入网络并对有线和无线网络的访问执行设备身份验证。网络访问管理器对安全访问所需的用户及设备身份和网络访问协议进行管理。智能化地工作可防止最终用户进行违反管理员定义的策略的连接。

网络访问管理器采用单宿主设计，一次只允许一个网络连接。此外，有线连接具有高于无线连接的优先级，因此，如果将您插入包含有线连接的网络，则无线适配器将变为禁用状态，并且没有 IP 地址。

如果您的有线或无线网络设置或特定 SSID 从组策略推送，它们可能会与网络访问管理器的正常运行冲突。在安装了网络访问管理器的情况下，不支持无线设置的组策略。

注释 网络访问管理器在 macOS 或 Linux 上不支持。

注释 如果在 Windows OS 上使用 ISE 终端安全评估，则必须在启动 AnyConnect ISE 终端安全评估之前安装网络访问管理器。

Cisco AnyConnect Secure Mobility Client的网络访问管理器组件支持以下主要功能：

- 传输层安全 (TLS) 协议版本 1.2
- 有线 (IEEE 802.3) 和无线 (IEEE 802.11) 网络适配器。

- 一些搭配 Windows 7 或更高版本的移动宽带 (3G) 网络适配器。（需要支持 Microsoft 移动宽带 API 的 WAN 适配器。）
- 使用 Windows 机器凭证的登录前身份验证。
- 使用 Windows 登录凭证的单点登录用户身份验证。
- 简化的 IEEE 802.1X 配置。
- IEEE MACsec 有线加密和企业策略控制。
- EAP 方法：
  - EAP-FAST、PEAP、EAP-TTLS、EAP-TLS 和 LEAP（EAP-MD5、EAP-GTC 和仅用于 IEEE 802.3 有线的 EAP-MSCHAPv2）。
- 内部 EAP 方法：
  - PEAP - EAP-GTC、EAP-MSCHAPv2 和 EAP-TLS。
  - EAP-TTLS - EAP-MD5 和 EAP-MSCHAPv2 和传统方法（PAP、CHAP、MSCHAP 和 MSCHAPv2）。
  - EAP-FAST - GTC、EAP-MSCHAPv2 和 EAP-TLS。
- 加密模式 - 静态 WEP（打开或共享）、动态 WEP、TKIP 和 AES。
- 密钥建立协议 - WPA、WPA2/802.11i。
- AnyConnect 在以下环境中支持提供智能卡的凭证：
  - Windows 中的 Microsoft CAPI 1.0 和 CAPI 2.0 (CNG)。
  - Windows 登录不支持 ECDSA 证书。因此，网络访问管理器单点登录 (SSO) 不支持 ECDSA 客户端证书。

注释 WPA3 目前不支持。

套件 B 和 FIPS

以下功能已在 Windows 7 或更高版本上经过 FIPS 认证，并且列出了所有例外情况：

- ACS 和 ISE 不支持 Suite B，但具有 OpenSSL 1.x 的 FreeRADIUS 2.x 支持 Suite B。Microsoft NPS 2008 部分支持 Suite B（NPS 证书仍必须是 RSA）。
- 802.1X/EAP 只支持过渡性 Suite B 配置文件（如 RFC 5430 中定义）。
- MACsec 符合 FIPS 规范。
- 支持 Elliptic Curve Diffie-Hellman (ECDH) 密钥交换。

- 支持 ECDSA 客户端证书。
- 支持操作系统存储区中的 ECDSA CA 证书。
- 支持网络配置文件中的 ECDSA CA 证书（PEM 编码）。
- 支持服务器的 ECDSA 证书链验证。

单点登录“单一用户”实施

Microsoft Windows 允许多名用户同时登录，但思科 AnyConnect 网络访问管理器将网络身份验证仅限于对单一用户执行。无论有多少用户登录，AnyConnect 网络访问管理器都在每个桌面或每台服务器上为一位用户保持活动状态。单用户登录实施意味着只有一位用户可以随时登录到系统，并且管理员无法强制当前登录的用户注销。

如果网络访问管理器客户端模块安装在 Windows 桌面上，系统的默认行为是实施单一用户登录。如果该模块安装在服务器上，默认行为是解除单一用户登录实施。但无论是哪种情况，您都可修改或添加注册表来更改默认行为。

限制

- Windows 管理员无法强制注销当前登录的用户。
- 对于同一用户，支持与所连接工作站的 RDP 会话。
- 凭证格式相同才会被视为同一用户。例如，user/example 与 user@example.com 就不相同。
- 智能卡用户也必须确保 PIN 相同才会被视为同一用户。

配置单点登录单一用户实施

要更改 Windows 工作站或服务器处理多位用户的方式，请更改注册表中 EnforceSingleLogon 的值。

在 Windows 中，该注册表项是 **EnforceSingleLogon** 且与 OverlayIcon 项在同一注册表位置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Providers\{B12744B8-5BB7-463a-B85E-BB7627E73002}
```

要配置一位或多位用户登录，请添加名为 EnforceSingleLogon 的 DWORD，并为其赋值 1 或 0。

对于 Windows：

- 1 表示仅限一个用户登录。
- 0 允许多位用户进行登录。

网络访问管理器部署

网络访问管理器作为 AnyConnect 的一部分进行部署。有关如何安装 AnyConnect 以及网络访问管理器和其他模块的信息，请参阅 AnyConnect 部署概述。

指南

- Windows 网络状态任务托盘图标引起的困扰 - 网络访问管理器将覆盖 Windows 网络管理。因此，在安装网络访问管理器后，无法使用网络状态图标连接到网络。

  建议操作：通过在 Windows 组策略中设置**删除网络图标**来删除任务托盘中的 Windows 网络图标。此设置仅影响托盘图标。用户仍可以使用控制面板创建本地无线网络。

- Windows 7 或更高版本的隐藏网络和网络选择 - 网络访问管理器尝试只连接在网络访问管理器网络扫描列表中配置的网络。

  在 Windows 7 或更高版本中，网络访问管理器会探测隐藏的 SSID。当发现第一个隐藏的 SSID 后，即停止查找。当配置了多个隐藏网络时，网络访问管理器按如下方式选择 SSID：

  - 第一个管理员定义的隐藏企业网络。
  - 管理员定义的隐藏网络。
  - 第一个用户定义的隐藏网络。由于网络访问管理器一次只能探测一个非广播 SSID，因此思科建议在您的站点只使用一个隐藏的企业网络。

- 网络连接短暂丢失或更长的连接时间 - 如果在安装网络访问管理器之前在 Windows 中定义了网络，Windows 连接管理器可能偶尔尝试与该网络建立连接。

  建议操作：当网络在范围内时，对所有 Windows 定义的网络关闭**自动连接 (Connect Automatically)** 或删除所有 Windows 定义的网络。

- 当网络访问管理器模块首次安装到客户端系统时，该模块可以配置为将一些现有 Windows 7 或更高版本无线配置文件转换为网络访问管理器配置文件格式。可以转换匹配以下条件的基础设施网络：

  - 开放
  - 静态 WEP
  - WPA/WPA2 个人
  - 只转换非 GPO 本地 Wi-Fi 用户网络配置文件。
  - 在配置文件转换期间，系统上必须运行 WLAN 服务。
  - 如果网络访问管理器 XML 配置文件已存在 (userConfiguration.xml)，则不会进行转换。

  要启用网络配置文件转换，请创建一个 MSI 转换将 PROFILE_CONVERSION 属性值设置为 1，然后将其应用到 MSI 包。或者在命令行中将 PROFILE_CONVERSION 属性更改为 1，然后安装 MSI 包。例如，**msiexec /i anyconnect-nam-win-3.1.xxxxx-k9.msi PROFILE_CONVERSION=1**。

- 必须先安装网络访问管理器，再启动 ISE 终端安全评估。ISE 终端安全评估使用网络访问管理器插件检测网络更改事件和 802.1x WiFi。

禁用 DHCP 连接性测试

当网络配置为使用动态 IP 地址时，Windows OS 服务尝试使用 DHCP 建立连接。然而，在通知网络访问管理器 DHCP 事务已完成之前，该操作系统的过程可能需要长达两分钟。除了 OS DHCP 事务外，网络访问管理器还触发了 DHCP 事务，以避免在通过操作系统建立连接时出现较大延迟并检验网络连接。

当您想要通过 NAM 禁用 DHCP 事务来进行连接测试，请添加以下注册表项为 DWORD，然后将数值进行如下设置：

- 64 位 Windows - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\Cisco AnyConnect Network Access Manager\DisableDHCP 设置为 1
- 32 位 Windows - HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Network Access Manager\DisableDHCP 设置为 1

注释 我们强烈建议您不要禁用网络访问管理器 DHCP 连接性测试，因为它常常导致连接时间延长。

网络访问管理器配置文件

网络访问管理器配置文件在网络访问管理器配置文件编辑器中进行配置，后者在 ASDM 中提供，也可以作为独立的 Windows 应用。

“客户端策略”(Client Policy) 窗口

客户端策略 (Client Policy) 窗口可用于配置客户端策略选项。包括以下部分：

连接设置

可用于定义是在用户登录之前还是之后尝试建立网络连接。

- **默认连接超时 (Default Connection Timeout)** - 用作用户创建的网络的连接超时秒数。默认值是 40 秒。
- **用户登录前 (Before User Logon)** - 在用户登录之前连接网络。支持的用户登录类型包括用户帐户 (Kerberos) 身份验证，加载用户 GPO 和执行基于 GPO 的登录脚本。如果选择了“用户登录前”(Before User Logon)，您还可以设置允许用户登录前等待的时间 *(Time to Wait Before Allowing a User to Logon)*。

- **允许用户登录前等待的时间 (Time to wait before allowing user to Logon)** - 指定等待网络访问管理器建立完整网络连接的最大秒数（最坏情况）。如果无法在此时间内建立网络连接，则Windows登录进程继续进行用户登录。默认值为 5 秒。

  注释 如果网络访问管理器配置为管理无线连接，则必须将**允许用户登录前等待的时间 (Time to wait before allowing user to Logon)**设置为30秒或更长时间，因为可能还要额外花时间来建立无线连接。您还应该考虑到通过 DHCP 获取 IP 地址所需的时间。如果配置了两个或更多网络配置文件，您应该增大此值以涵盖两次或更多次连接尝试。

- **用户登录后 (After User Logon)** - 在用户登录到 Windows 之后连接网络。

媒体

指定哪些类型的媒体由网络访问管理器客户端控制。

- **管理 Wi-Fi（无线）媒体 (Manage Wi-Fi [wireless] Media)** - 启用 Wi-Fi 媒体的管理和 WPA/WPA2 握手的验证（可选）。

  IEEE 802.11i 无线网络标准指定请求方（在本例中是网络访问管理器）必须验证接入点的 RSN IE（即稳健的安全网络信息交换）。IE 是在密钥派生期间放在IEEE 801.X 协议数据包的 EAPOL 密钥数据中发送的，它应该与信标/探针响应帧中接入点的 RSN IE 匹配。

- **启用 WPA/WPA2 握手的验证 (Enable validation of WPA/WPA2 handshake)** - 验证 WPA/WPA2 握手。如果未选中，则跳过此可选验证步骤。

  注释 某些适配器并不一直提供接入点的RSN IE，因此身份验证尝试失败，客户端将无法连接。

- **默认关联超时 (Default Association Timeout)**（秒）- 如果启用 WPA/WPA2 握手，则必须指定默认关联超时。
- **管理有线 (IEEE 802.3) 媒体 (Manage Wired [IEEE 802.3] Media)** - 启用有线连接的管理。
- **管理移动宽带介质 (Manage Mobile Broadband Media)** - 启用 Windows Mobile 宽带适配器的管理。此功能默认为已禁用。

  注释 此功能处于试用版本状态。思科 TAC 对试用版本不提供支持。

- **启用数据漫游 (Enable Data Roaming)** - 确定是否允许数据漫游。

最终用户控制

可以为用户配置以下控制：

- **禁用客户端 (Disable Client)** - 允许用户禁用和启用使用 AnyConnect UI 进行网络访问管理器的有线和无线媒体管理。
- **显示用户组 (Display user groups)** - 让用户创建的组（从 CSSC 5.x 创建）可见且能够连接，即使它们并不是管理员定义的组也是如此。
- **指定连接时运行的脚本或应用 (Specify a script or application to run when connected)** - 允许用户指定网络连接时运行的脚本或应用。

  注释 脚本设置特定于一个用户配置的网络，并允许用户指定当该网络处于连接状态时运行的本地文件（.exe、.bat 或 .cmd）。为避免冲突，此脚本功能允许用户只为用户定义的网络（而不为管理员定义的网络）配置脚本或应用。此功能不允许用户就脚本运行而更改管理员网络。因此，管理员网络界面对用户不可用。此外，如果不允许用户配置正在运行的脚本，则此功能不会出现在网络访问管理器 GUI 中。

- **自动连接 (Auto-connect)** - 自动连接到一个网络，无需用户选择它。默认值为自动连接。

管理状态

- **服务操作 (Service Operation)** - 如果关闭服务，则使用此配置文件的客户端将无法连接以建立第二层连接。
- **FIPS 模式 (FIPS Mode)** - 如果启用 FIPS 模式，则网络访问管理器以符合政府要求的方式执行密码操作。

  联邦信息处理标准（FIPS 140-2 级别 1）是指定加密模块的安全要求的美国政府标准。根据软件和硬件的类型，FIPS 由面向 MACsec 或 Wi-Fi 的网络访问管理器支持。

  表 *6:* 网络访问管理器的 *FIPS* 支持

媒体/操作系统	Windows 7 或更高版本
MACsec 有线网络	当使用支持 MACsec 的英特尔硬件 NIC 或任何非硬件 MACsec 时，都符合 FIPS。
Wi-Fi	不兼容的 FIPS

“身份验证策略”(Authentication Policy) 窗口

Authentication Policy 窗口可用于创建关联和身份验证网络过滤器，这些过滤器适用于所有网络连接。如果未选中任何关联或身份验证模式，则用户无法连接到身份验证 Wi-Fi 网络。如果选择了模式的

子集，则用户仅能连接到这些类型的网络。选择每个所需的关联或身份验证模式，或者选择**全选 (Select All)**。

内部方法也可以仅限于特定的身份验证协议。内部方法缩进显示在 Allowed Authentication Modes 窗格中外部方法（隧道）的下面。

选择身份验证协议的机制与当前客户端身份验证数据库集成在一起。安全无线局域网部署不要求为用户创建新的身份验证系统。

对内部隧道可用的 EAP 方法取决于内部方法凭证类型和外部隧道方法。在以下列表中，每个外部隧道方法都列出了针对每种凭证类型受支持的内部方法类型。

- PEAP
  - 密码凭证：EAP-MSCHAPv2 或 EAP-GTC
  - 令牌凭证：EAP-GTC
  - 证书凭证：EAP-TLS
- EAP-FAST
  - 密码凭证：EAP-MSCHAPv2 或 EAP-GTC
  - 令牌凭证：EAP-GTC
  - 证书凭证：EAP-TLS
- EAP-TTLS
  - 密码凭证：EAP-MSCHAPv2、EAP-MD5、PAP（传统）、CHAP（传统）、MSCHAP（传统）、MSCHAP-v2（传统）
  - 令牌凭证：PAP（传统）。网络访问管理器支持的默认令牌选项是 PAP，因为质询/响应方法并不是很适合基于令牌的身份验证。
  - 证书凭证：不适用

“网络”(Networks) 窗口

Networks 窗口可用于为企业用户配置预定义的网络。您可以配置对所有组可用的网络，或创建具有特定网络的组。“网络”(Networks) 窗口显示向导，可将窗格添加到现有窗口中，并且可让您通过单击**下一步 (Next)** 访问更多配置选项。

从根本上说，组是一套配置的连接（网络）。每个已配置的连接必须属于某个组，或者是所有组的成员。

注释 为向后兼容，使用思科安全服务客户端部署的由管理员创建的网络被视为隐藏的网络，不广播SSID。但是，用户网络被视为广播 SSID 的网络。

只有管理员可以创建新组。如果配置中未定义组，配置文件编辑器会创建一个自动生成的组。自动生成的组中包含未分配到任何管理员定义的组的网络。客户端尝试使用在活动组中定义的连接创建网络连接。根据“网络组”(Network Groups) 窗口中**创建网络 (Create Networks)** 选项的设置，最终用户可以将用户网络添加到活动组，或者从活动组删除用户网络。

定义的网络可用于列表顶部的所有组。因为您控制哪些网络位于全球网络中，所以您可以指定最终用户能够连接的网络，即使存在用户定义的网络也一样。最终用户无法修改或删除管理员配置的网络。

注释 最终用户可以将网络添加到组，但全球网络部分的网络除外，因为这些网络存在于所有组中，只能使用配置文件编辑器创建。

企业网络的典型最终用户不需要了解组即可使用此客户端。活动组是配置中的第一个组，但如果只有一个组可用，客户端不会知道活动组，也不会显示活动组。但是，如果存在多个组，用户界面会显示组的列表，并且指示活动组已选中。然后，用户可以从活动组中选择，重启后该设置也保持不变。根据“网络组”(Network Groups) 窗口中**创建网络 (Create Networks)** 选项的设置，最终用户无需使用组即可添加或删除自己的网络。

注释 组选择在重启和网络修复（右键单击托盘图标并选择**网络修复 (Network Repair)** 来完成）后保持不变。网络访问管理器在修复或重新启动时，会开始使用以前的活动组。

“网络”(Networks) 窗口的“媒体类型”(Media Type) 页面

您可以在 Networks 窗口的 Media Type 页面中创建或编辑有线或无线网络。设置随您的具体选择而不同。

第一个对话框中包括以下部分：

- Name - 输入将为该网络显示的名称。
- 组成员 (Group Membership) - 选择此配置文件应该对哪些网络组或组可用。
- 网络媒体 (Network Media) - 选择有线或 Wi-Fi（无线）。如果选择 Wi-Fi，您还可以配置以下参数：
  - SSID - 输入您的无线网络的 SSID（服务集标识符）。
  - Hidden Network - 允许连接到网络，即使它不广播其 SSID。
  - Corporate Network - 如果附近有企业网络，强制将网络连接首先配置为 Corporate。当企业网络使用非广播（隐藏）SSID 并且配置为隐藏时，网络访问管理器会主动寻找隐藏的 SSID，并且当有企业 SSID 在范围内时建立连接。
  - Association Timeout - 输入网络访问管理器在重新评估可用网络之前等待与特定无线网络相关联的时长。默认的关联超时为 5 秒。

- 常用设置
  - 脚本或应用程序 (Script or application) - 输入将在本地系统中运行的文件的路径和文件名，或者浏览文件夹并选择一个文件。以下规则适用于脚本和应用：
    - 您无法在登录前启动模式下运行脚本。
    - 接受扩展名为 .exe、.bat 或 .cmd 的文件。
    - 用户不得更改管理员创建的网络中定义的脚本或应用。
    - 您可以使用配置文件编辑器仅指定路径和脚本或应用的文件名。如果脚本或应用不存在于用户的机器上，将会显示一条错误消息。用户获通知，脚本或应用不存在于其机器上，并且需要联系系统管理员。
    - 您必须指定要运行的应用的完整路径，除非应用存在于用户的路径中。如果应用存在于用户的路径中，您可以仅指定应用或脚本的名称。
    - Connection Timeout - 输入网络访问管理器尝试连接到其他网络（当连接模式为自动时）或者使用另一个适配器之前等待建立网络连接的秒数。

注释 某些智能卡身份验证系统需要近 60 秒才能完成身份验证。使用智能卡时，您应增加 Connection Timeout 值，尤其是当智能卡可能必须尝试几个网络才能连接成功时。

注释 为了缓解在特定智能卡中间件上发现的问题，AnyConnect 网络访问管理器通过对测试数据执行签名操作并验证该签名来验证智能卡 PIN。此测试签名针对位于智能卡上的每个证书进行，并且与证书的数量有关，因此可能显著增加智能卡身份验证的延迟。如果要禁用测试签名操作，可以在 HKEY_LOCAL_MACHINE/SOFTWARE/Cisco/Cisco AnyConnect Network Access Manager 中将 **DisableSmartcardPinVerifyBySigning** 作为一个 DWORD 添加到注册表项中并将其设置为 1。对启用此注册表项的任何更改都应使用所有智能卡和相关硬件进行全面测试，以确保操作正确。

“网络”(Networks) 窗口的“安全等级”(Security Level) 页面

在“网络”(Networks) 向导的“安全等级”(Security Level) 页面中，选择“开放式网络”(Open Network)、“身份验证网络”(Authentication Network) 或（仅为无线网络介质显示的）“共享密钥网络”(Shared Key Network)。每种网络类型的配置流程都不同，在以下各节进行说明。

- 配置身份验证网络 - 建议用于安全企业。
- 配置开放网络 - 不推荐，但是可用于通过强制网络门户环境提供访客接入。在强制网络门户状态下，网络访问管理器不支持自动启动浏览器。
- 配置共享密钥网络 - 建议用于小型办公室或家庭办公室等无线网络。

配置身份验证网络

如果您在“安全级别”(Security Level) 部分选择“身份验证网络”(Authenticating Network)，将显示额外的窗格，如下所述。在这些窗格中完成配置后，请单击**下一步 (Next)** 按钮，或选择**连接类型 (Connection Type)**选项卡打开“网络连接类型”(Network Connection Type) 对话框。

802.1X Settings 窗格

根据网络配置调整 IEEE 802.1X 设置：

注释 当 AnyConnect ISE 终端安全评估安装了网络访问管理器时，ISE 终端安全评估使用网络访问管理器插件检测到网络更改事件和 802.1X WiFi。

- authPeriod（秒）- 身份验证开始时，此设置将确定在身份验证消息超时之前请求方等待的时长，该时间过后需要验证方重新发起身份验证。
- heldPeriod（秒）- 身份验证失败时，此设置定义请求方等待多长时间后才能发出另一次身份验证尝试。
- startPeriod（秒）- 没有从验证方收到对 EAPOL-Start 消息的任何响应时，再次传输 EAPOL-Start 消息之间的时间间隔（秒）。
- maxStart - 请求方通过发送 IEEE 801.X 协议数据包、EAPOL 密钥数据或 EAPoL-Start，向验证方发起身份验证的次数，达到此次数后，请求方会假定没有验证方。此时，请求方允许数据流量。

提示 您可以仔细设置 startPeriod 和 maxStart，使发起身份验证所花的总时间小于网络连接计时器时间（startPeriod x maxStart < 网络连接计时器时间），配置单一身份验证有线连接以同时支持开放网络和身份验证网络。

请注意，在这种情况下，您应将网络连接计时器时间增加 (startPeriod x maxStart) 秒，让客户端有足够的时间获取 DHCP 地址和完成网络连接。

相反，若要仅在身份验证成功后才允许数据流量，您应该设置 startPeriod 和 maxStart，确保发起身份验证所花的总时间大于网络连接计时器时间（startPeriod x maxStart > 网络连接计时器时间）。

Security 窗格

仅为有线网络显示。

在“安全”(Security) 窗格中，选择以下参数的值：

- Key Management - 确定哪个密钥管理协议用于启用 MACsec 的有线网络。
  - None - 没有使用密钥管理协议，并且不执行有线加密。
  - MKA - 请求方尝试协商 MACsec 密钥管理协议策略和加密密钥。MACsec 是 MAC 层安全，在有线网络上提供 MAC 层加密。MACsec 协议采用加密手段来保护 MAC 层帧，依靠 MACsec 密钥协议 (MKA) 实体进行协商并分发加密密钥。
- 加密
  - None - 对数据流量执行完整性检查，但不加密。
  - MACsec: AES-GCM-128 - 仅当选择 MKA 进行密钥管理时，此选项才可用。它会使用 AES-GCM-128 对数据流量进行加密。
  - MACsec: AES-GCM-256 - 具有企业边缘 (eEdge) 集成的选定 IOS 版本支持此选项，仅当您选择 MKA 进行密钥管理时才可使用此选项。它必须与交换机端的设置匹配。通过启用 MACsec 256 加密标准，下行链路端口支持具有 MACsec 密钥协议 (MKA) 的 802.11 AE 加密，以便在具有 MACsec 功能的设备和主机设备之间进行加密。

有关详细信息，请参阅基于身份的网络服务：MAC 安全。

Port Authentication Exception Policy 窗格

此窗格仅为有线网络显示。

Port Authentication Exception Policy 窗格可让您在身份验证过程中定制 IEEE 802.1X 请求方的行为。如果端口异常未启用，请求方会继续其现有行为并仅在成功完成完整配置后（或如此部分之前所述，发起身份验证的 maxStarts 数量而没有验证器响应之后）才会打开端口。选择以下其中一个选项：

- 在身份验证前允许数据流量通过 - 在身份验证尝试之前允许数据流量通过。
- 在身份验证之后允许数据流量通过，即使：
  - EAP 失败 - 选择后，请求方尝试身份验证。如果身份验证失败，请求方在身份验证失败的情况下依然允许数据流量通过。
  - EAP 成功，但密钥管理失败 - 选择后，请求方尝试与密钥服务器就密钥进行协商，但在密钥协商因任何原因失败的情况下依然允许数据流量通过。此设置仅在已配置密钥管理的情况下有效。如果密钥管理设置为无，则复选框以灰色显示。

限制 MACsec 需要 ACS 版本 5.1 及更高版本和支持 MACsec 的交换机。请参阅《*Catalyst 3750-X* 和 *3560-X* 交换机软件配置指南》以了解 ACS 或交换机配置。

关联模式

该窗格仅对无线网络显示。

选择关联模式：

- WEP
- WAP Enterprise (TKIP)
- WPA Enterprise (AES)
- WPA 2 Enterprise (TKIP)
- WPA 2 Enterprise (AES)
- CCKM (TKIP) -（需要思科 CB21AG 无线网卡）
- CCKM (AES) -（需要思科 CB21AG 无线网卡）

配置开放网络

开放网络不使用身份验证或加密。如果要创建开放（非安全）网络，请执行以下步骤。

步骤 1 从 Security Level 页面选择**开放式网络 (Open Network)**。此选择提供的网络安全性最低，建议用于访客接入无线网络。

步骤 2 单击**下一步 (Next)**。

步骤 3 确定连接类型。

配置共享密钥网络

Wi-Fi网络可使用共享密钥获得加密密钥，用于在终端之间和网络接入点之间对数据加密。配合WPA或 WPA2 Personal 使用共享密钥，可提供中等级别的安全性，适合于小型或家庭办公室。

注释 不建议对企业无线网络使用共享密钥安全性。

如果要将共享密钥网络作为您的安全级别，请执行以下步骤。

步骤 1 选择**共享密钥网络 (Shared Key Network)**。

步骤 2 在“安全级别”(Security Level) 窗口中单击**下一步 (Next)**。

步骤 3 指定 **User Connection** 或 **Machine Connection**。

步骤 4 单击**下一步 (Next)**。

步骤 5 Shared Key Type - 指定共享密钥关联模式，用于确定共享密钥类型。选项如下所示：

- WEP - 与静态 WEP 加密关联传统 IEEE 802.11 开放系统。
- Shared - 与静态 WEP 加密关联传统 IEEE 802.11 共享密钥。

- WPA/WPA2-Personal - 一种 Wi-Fi 安全协议，用于从密码预共享密钥 (PSK) 获得加密密钥。

步骤 6 如果选择了传统 IEEE 802.11 WEP 或共享密钥，请选择 40 位、64 位、104 位或 128 位。40 位或 64 位 WEP 密钥必须是 5 个 ASCII 字符或 10 个十六进制数字。104 位或 128 位 WEP 密钥必须是 13 个 ASCII 字符或 26 个十六进制数字。

步骤 7 如果选择了 WPA 或“WPA2 个人”(WPA2 Personal)，请选择要使用的加密类型 (TKIP/AES)，然后输入共享密钥。输入的密钥必须为 8 到 63 个 ASCII 字符或正好 64 个十六进制数字。如果共享密钥由 ASCII 字符组成，请选择 **ASCII**。如果共享密钥包含 64 个十六进制数字，请选择**十六进制 (Hexadecimal)**。

步骤 8 单击**完成 (Done)**。然后单击**确定 (OK)**。

Networks， Network Connection Type 窗格

本节介绍 Networks 窗口的网络连接类型窗格，该窗格遵循网络访问管理器配置文件编辑器中的安全级别。选择以下连接类型之一：

- Machine Connection - 存储在 Windows Active Directory 中的设备名称用来进行授权。计算机连接通常用于无需用户凭证进行连接的情况。即使用户已注销且用户凭证不可用，如果终端站应登录到网络，也请选择此选项。此选项通常用于在用户获得访问权限之前连接域并从网络获得 GPO 和其他更新。

  注释 如果没有可用的已知网络，VPN 登录前启动 (SBL) 会失败。SBL 模式中允许的网络配置文件包括使用非 802-1X 身份验证模式的所有媒体类型，例如开放 WEP、WPA/WPA2 个人和静态密钥 (WEP) 网络。如果为 Before User Logon 和计算机连接授权配置网络访问管理器，网络访问管理器将要求用户提供网络信息，并且 VPN SBL 成功启动。

- User Connection - 用户凭证用于进行授权。

  如果在“客户端策略”(Client Policy) 窗格中选择了“用户登录前”(Before User Logon)，则用户在 Windows 开始屏幕中输入登录凭证后，网络访问管理器会收集用户的凭证。在 Windows 启动用户的 Windows 会话时，网络访问管理器会建立网络连接。

  如果在“客户端策略”(Client Policy) 窗格中选择了“用户登录后”(After User Logon)，则用户登录到 Windows 后，网络访问管理器才启动连接。

  用户注销后，当前用户网络连接即终止。如果计算机网络配置文件可用，NAM 会重新连接到计算机网络。

- Machine and User Connection - 仅在配置网络身份验证时可用，如在 Security Level 窗格中所选。计算机 ID 和用户凭证均使用，但仅当用户未登录到设备时，计算机部分才有效。这两部分的配置是相同的，但是，计算机连接的身份验证类型和凭证可能与用户连接的身份验证类型和凭证不同。

当用户未登录时，选择此选项可始终通过计算机连接将 PC 连接到网络。当用户已登录时，选择此选项可始终通过用户连接将 PC 连接到网络。

在 EAP-FAST 配置为 EAP 方法（在下一个窗格中）时，支持 EAP 链接。这意味着网络访问管理器会确认计算机和用户为已知实体并且由公司管理。

当您选择网络连接类型时，“网络”(Networks) 对话框中会显示其他选项卡。使用这些选项卡，可为所选网络连接类型设置 EAP 方法和凭证。

Networks、User 或 Machine Authentication 页面

在选择网络连接类型后，选择这些连接类型的身份验证方法。在选择身份验证方法后，显示屏幕会更新为选择的方法，并要求您提供其他信息。

注释 如果您已启用 MACsec，请确保选择支持 MSK 密钥派生的 EAP 方法，例如 PEAP、EAP-TLS 或 EAP-FAST。此外，即使没有启用 MACsec，使用网络访问管理器也可将 MTU 从 1500 降低至 1468 以支持 MACsec。

EAP 概述

EAP 是一种 IETF RFC，可满足身份验证协议与承载它的传输协议进行分离的要求。此分离允许传输协议（如 IEEE 802.1X、UDP 或 RADIUS）承载 EAP 协议，而无需更改身份验证协议。

基本 EAP 协议包括四种数据包类型：

- EAP 请求 - 身份验证器向请求方发送请求数据包。每个请求都有一个类型字段，用于指示请求内容，如请求方身份和要使用的 EAP 类型。顺序号允许身份验证器和对等项将 EAP 响应与各个 EAP 请求进行匹配。
- EAP 响应 - 请求方向身份验证器发送响应数据包并使用顺序号与启动的 EAP 请求进行匹配。EAP 响应的类型通常匹配 EAP 请求，除非响应为负 (NAK)。
- EAP 成功 - 身份验证成功后，身份验证器向请求方发送成功数据包。
- EAP 失败 - 如果身份验证失败，身份验证器向请求方发送失败数据包。

在 IEEE 802.11X 系统中使用 EAP 时，接入点在 EAP 穿透模式下工作。在此模式下，接入点检查代码、标识符和长度字段，然后将从请求方收到的 EAP 数据包转发至 AAA 服务器。从 AAA 服务器身份验证器接收的数据包将转发到请求方。

EAP-GTC

EAP-GTC 是基于简单用户名和密码身份验证的 EAP 身份验证方法。不使用质询响应方法，用户名和密码均以明文传递。建议在隧道 EAP 方法内部（请参阅下面的隧道 EAP 方法）或针对一次性密码 (OTP) 使用此方法。

EAP-GTC 不提供相互身份验证。它只对客户端进行身份验证，因此欺诈服务器可能会获取用户的凭证。如果需要相互身份验证，则在隧道 EAP 方法内部使用 EAP-GTC，这样可提供服务器身份验证。

EAP-GTC 未提供密钥材料。因此，不能对 MACsec 使用此方法。如果进一步的流量加密需要密钥材料，则在隧道 EAP 方法内使用 EAP-GTC，这样可提供密钥材料（如有必要，还提供内部和外部 EAP 方法加密绑定）。

有两个密码源选项：

- 使用密码进行身份验证 - 只适用于有良好保护的有线环境
- 使用令牌进行身份验证 - 更安全，因为令牌代码或 OTP 的生命期较短（通常约为 10 秒）

注释 网络访问管理器、身份验证器和 EAP-GTC 协议均无法区分密码和令牌代码。这些选项只影响网络访问管理器中凭证的生命期。虽然可在注销前或更长时间内记住密码，但不能记住令牌代码（因为每次身份验证时都提示用户输入令牌代码）。

如果使用密码进行身份验证，可以使用此协议对照包含哈希值密码的数据库进行身份验证，因为密码以明文传递到身份验证器。如果存在数据库泄露的可能，建议使用此方法。

EAP-TLS

EAP 传输层安全 (EAP-TLS) 是基于 TLS 协议 (RFC 2246) 的 IEEE 802.1X EAP 身份验证算法。TLS 使用基于 X.509 数字证书的相互身份验证。EAP-TLS 消息交换提供相互身份验证、加密套件协商、密钥交换、客户端与身份验证服务器之间的身份验证以及可用于流量加密的密钥材料。

下面的列表提供了 EAP-TLS 客户端证书可为有线和无线连接提供强身份验证的主要原因：

- 身份验证自动进行，通常无需用户干预。
- 不存在对用户密码的依赖性。
- 数字证书提供强身份验证保护。
- 使用公共密钥加密保护消息交换。
- 证书不易受字典攻击。
- 身份验证过程会为数据加密和签名生成相互确定的密钥。

EAP-TLS 包含两个选项：

- “验证服务器证书”(Validate Server Certificate) - 启用服务器证书验证。
- “启用快速重新连接”(Enable Fast Reconnect) - 启用 TLS 会话恢复，只要 TLS 会话数据同时保存在客户端和服务器上，就允许使用简短的 TLS 握手进行快得多的重新身份验证。

注释 对于计算机连接身份验证，“使用智能卡时禁用”(Disable When Using a Smart Card) 选项不可用。

EAP-TTLS

EAP 隧道传输层安全 (EAP-TTLS) 是扩展 EAP-TLS 功能的两阶段协议。第 1 阶段执行完整 TLS 会话，并生成用于在第 2 阶段安全地在服务器与客户端之间隧道化属性的会话密钥。您可以使用在第 2 阶段隧道化的属性通过多种不同机制执行其他身份验证。

网络访问管理器不支持在 EAP-TTLS 身份验证期间使用的内部和外部方法加密绑定。如果需要加密绑定，则必须使用 EAP-FAST。加密绑定可防御特殊类别的中间人攻击，在这类攻击中，攻击者无需知道凭证就可以劫持用户的连接。

可以在第 2 阶段使用的身份验证机制包括以下协议：

- PAP（密码验证协议）- 使用双向握手为对等项提供证明其身份的简单方法。对等项向身份验证器重复发送 ID/密码对，直至身份验证确认或失败。如果需要相互身份验证，必须将 EAP-TTLS 配置为在第 1 阶段验证服务器证书。

  由于密码传递到身份验证器，您可以使用此协议对照包含哈希值密码的数据库进行身份验证。如果存在数据库泄露的可能，建议使用此方法。

  注释 可以使用 EAP-TTLS PAP 进行基于令牌和基于 OTP 的身份验证。

- CHAP（质询握手身份验证协议）- 使用三次握手验证对等项的身份。如果需要相互身份验证，应将 EAP-TTLS 配置为在第 1 阶段验证服务器证书。使用此质询响应方法，需要在身份验证器的数据库中存储明文密码。
- MS-CHAP (Microsoft CHAP) - 使用三次握手验证对等项的身份。如果需要相互身份验证，应将 EAP-TTLS 配置为在第 1 阶段验证服务器证书。使用这个基于密码的 NT 哈希值的质询响应方法，需要在身份验证器的数据库中存储明文密码或至少存储密码的 NT 哈希值。
- MS-CHAPv2 - 通过在响应数据包中包含对等项质询以及在成功数据包中包含身份验证器响应来提供对等项之间的相互身份验证。先对客户端、再对服务器进行身份验证。如果服务器需要先于客户端进行身份验证（以防御字典攻击），应该将 EAP-TTLS 配置为在第 1 阶段验证服务器证书。使用这个基于密码的 NT 哈希值的质询响应方法，需要在身份验证器的数据库中存储明文密码或至少存储密码的 NT 哈希值。

配置 EAP-TTLS

- EAP - 允许使用以下 EAP 方法之一：
  - EAP-MD5 (EAP Message Digest 5) - 使用三向握手来验证对等体的身份（类似于 CHAP）。使用这种质询-响应方法，需要在验证方的数据库中存储明文密码。

- EAP-MSCHAPv2 - 使用三次握手验证对等体的身份。先对客户端、再对服务器进行身份验证。如果对服务器的身份验证需要先于客户端（例如为防止字典攻击），则应配置EAP-TTLS以在第 1 阶段验证服务器的证书。对 NT 哈希值形式的密码使用这种质询-响应方法时，需要在验证方的数据库中存储明文密码或至少 NT 哈希值形式的密码。

- EAP-TTLS 设置
  - Validate Server Identity - 启用服务器证书验证。

    注释 如果启用此选项，请确保在 RADIUS 服务器上安装的服务器证书中包含服务器身份验证的扩展密钥用法 (EKU)。当 RADIUS 服务器在身份验证期间将其配置的证书发送到客户端时，必须对网络访问和身份验证使用此服务器身份验证设置。

  - Enable Fast Reconnect - 只启用外部 TLS 会话恢复，而不管内部身份验证是跳过还是由验证方控制。

    注释 Disable When Using a Smart Card 不适用于机器连接身份验证。

- Inner Methods - 指定在 TLS 隧道创建后使用的内部方法。仅适用于 Wi-Fi 媒体类型。

PEAP 选项

受保护的 EAP (PEAP) 是基于隧道 TLS 的 EAP 方法。它在客户端身份验证之前使用 TLS 进行服务器身份验证，以加密内部身份验证方法。内部身份验证在受信任加密保护的隧道内进行，支持多种不同的内部身份验证方法，包括证书、令牌和密码。网络访问管理器不支持在 PEAP 身份验证期间使用的内部和外部方法加密绑定。如果需要加密绑定，则必须使用 EAP-FAST。加密绑定可防御特殊类别的中间人攻击，在这类攻击中，攻击者无需知道凭证就可以劫持用户的连接。

PEAP 通过提供以下服务保护 EAP 方法：

- 为 EAP 数据包创建 TLS 隧道
- 消息身份验证
- 消息加密
- 服务器到客户端的身份验证

可以使用以下身份验证方法：

- 使用密码进行身份验证

- EAP-MSCHAPv2 - 使用三次握手验证对等体的身份。先对客户端、再对服务器进行身份验证。如果服务器需要先于客户端进行身份验证（如为了防御字典攻击），则必须配置PEAP以验证服务器的证书。使用基于密码的 NT 哈希值的质询响应方法，需要在身份验证器数据库中存储明文密码或至少存储密码的 NT 哈希值。
- EAP-GTC（EAP 通用令牌卡）- 定义 EAP 信封以承载用户名和密码。如果需要相互身份验证，则必须配置 PEAP 以验证服务器的证书。由于密码以明文传递到身份验证器，可以使用此协议对照包含哈希值密码的数据库进行身份验证。如果存在数据库泄露的可能，建议使用此方法。

- EAP-TLS，使用证书
  - EAP-TLS - 定义 EAP 信封以承载用户证书。为避免中间人攻击（劫持有效用户的连接），建议不要将 PEAP (EAP-TLS) 和 EAP-TLS 配置文件混合在一起向同一身份验证器进行身份验证。应相应地配置身份验证器（不同时启用普通和隧道 EAP-TLS）。

配置 PEAP

- PEAP-EAP 设置
  - Validate Server Identity - 启用服务器证书验证。

    注释 如果启用此选项，请确保在 RADIUS 服务器上安装的服务器证书中包含服务器身份验证的扩展密钥用法 (EKU)。当 RADIUS 服务器在身份验证期间将其配置的证书发送到客户端时，必须对网络访问和身份验证使用此服务器身份验证设置。

  - Enable Fast Reconnect - 仅启用外部 TLS 会话恢复。验证器控制是否跳过内部身份验证。
  - Disable when using a smart card - 在使用智能卡进行身份验证时，请勿使用“快速重新连接”。智能卡仅适用于用户连接。
  - Authenticate using a token and EAP GTC - 对计算机身份验证不可用。

- 基于凭证源的内部方法
  - 使用 EAP-MSCHAPv2 和/或 EAP-GTC 的密码进行身份验证。
  - EAP-TLS，使用证书进行身份验证。
  - 使用令牌和 EAP-GTC 进行身份验证 - 对计算机身份验证不可用。

    注释 在用户登录之前，智能卡支持在 Windows 上不可用。

EAP-FAST 设置

EAP-FAST 是 IEEE 802.1X 身份验证类型，可提供简单灵活的部署和管理。它支持多种用户和密码数据库类型、服务器发起的密码过期和更改以及数字证书（可选）。

EAP-FAST 针对想要部署 IEEE 802.1X EAP 类型的客户而开发，该类型不使用证书但可防御字典攻击。

自 AnyConnect 3.1 起，配置计算机和用户连接时均支持 EAP 链。这意味着网络访问管理器将验证计算机和用户是否为已知实体且由公司管理，这对于控制用户拥有的连接到企业网络的资产来说非常有用。有关 EAP 链的详细信息，请参阅 RFC 3748。

EAP-FAST 将 TLS 消息封装在 EAP 内，包括三个协议阶段：

1. 调配阶段 - 使用经过身份验证的 Diffie-Hellman 协议 (ADHP) 调配具有名为保护访问凭证 (PAC) 的共享加密凭证的客户端。
2. 隧道建立阶段 - 使用 PAC 建立隧道。
3. 身份验证阶段 - 身份验证服务器对用户凭证（令牌、用户名/密码或数字证书）进行身份验证。

与其他隧道 EAP 方法不同，EAP-FAST 提供内部和外部方法之间的加密绑定，可防御特殊类别的中间人攻击，在这类攻击中，攻击者可劫持有效用户的连接。

配置 EAP-FAST

- EAP-FAST 设置
  - Validate Server Identity - 启用服务器证书验证。启用此选项会在管理实用程序中引入两个额外的对话框，并且在网络访问管理器配置文件编辑器任务列表中添加额外的证书窗格。

    注释 如果启用此选项，请确保在 RADIUS 服务器上安装的服务器证书中包含服务器身份验证的扩展密钥用法 (EKU)。当 RADIUS 服务器在身份验证期间将其配置的证书发送到客户端时，必须对网络访问和身份验证使用此服务器身份验证设置。

  - Enable Fast Reconnect - 启用会话恢复。用来在 EAP-FAST 中恢复身份验证会话的两种机制是用户授权 PAC（用于代替内部身份验证）和 TLS 会话恢复（用于允许简化的外部 TLS 握手）。此 Enable Fast Reconnect 参数可启用或禁用这两种机制。验证方决定具体使用哪一种机制。

    注释 计算机 PAC 提供简化的 TLS 握手，无需内部身份验证。此控制通过启用/禁用 PAC 参数来处理。

注释 “使用智能卡时禁用”(Disable When Using a Smart Card) 选项仅适用于用户连接授权。

- Inner methods based on Credentials Source - 可让您使用密码或证书进行身份验证。
  - 使用 EAP-MSCHAPv2 或 EAP-GTC 的密码进行身份验证。EAP-MSCHAPv2 提供相互身份验证，但它先对客户端、再对服务器进行身份验证。如果要在相互身份验证中先对服务器进行身份验证，请配置 EAP-FAST 只用于经过身份验证的调配，并且验证服务器的证书。EAP-MSCHAPv2 使用基于密码的 NT 哈希值的质询-响应方法，它要求您在验证方的数据库中存储明文密码或至少 NT 哈希值形式的密码。由于密码在 EAP-GTC 中以明文形式传递给验证方，因此您可以使用此协议根据数据库进行身份验证。
  - Authenticate using a certificate - 决定使用证书进行身份验证的以下条件：收到请求时，以明文形式发送客户端证书，仅在隧道内发送客户端证书，或者使用 EAP-TLS 在隧道中发送客户端证书。
  - 使用令牌和 EAP-GTC 进行身份验证。
- Use PACs - 可以指定使用 PAC 进行 EAP-FAST 身份验证。PAC 是分发给客户端以优化网络身份验证的凭证。

注释 通常使用 PAC 选项，因为大多数身份验证服务器对 EAP-FAST 使用 PAC。在删除此选项之前，请验证身份验证服务器不对 EAP-FAST 使用 PAC。否则，客户端的身份验证尝试不会成功。

LEAP 设置

LEAP（轻量级 EAP）支持无线网络。它基于可扩展身份验证协议 (EAP) 框架，由思科开发，旨在创建比 WEP 更安全的协议。

注释 LEAP 容易受到字典攻击，除非实施强密码并定期使密码过期。思科建议使用 EAP-FAST、PEAP 或 EAP-TLS，它们的身份验证方法不易受字典攻击。

只能用于用户身份验证的 LEAP 设置：

- 注销后延长用户连接 - 用户注销后保持连接打开状态。如果同一用户再次登录，网络连接仍处于活动状态。

请参阅对 Cisco LEAP 漏洞的字典攻击以了解详细信息。

定义网络凭证

在 Networks > Credentials 窗格中，指定是否使用用户和/或机器凭证，并且配置受信任服务器验证规则。

配置用户凭证

EAP 对话可能涉及多种 EAP 身份验证方法，其中每种身份验证要求的身份可能不同（例如先是计算机身份验证，然后是用户身份验证）。例如，对等项最初可能声称身份为 nouser@cisco.com 以将身份验证请求发送到 cisco.com EAP 服务器。但是，一旦已协商 TLS 会话，对等项可能声称身份为 johndoe@cisco.com。因此，即使通过用户的身份提供保护，目标领域也不一定匹配，除非对话在本地身份验证服务器上终止。

对于用户连接，当使用了 [username] 和 [domain] 占位符模式时，适用以下条件：

- 如果客户端证书用于身份验证 - 从各 X509 证书属性获取 [username] 和 [password] 的占位符值。根据首次匹配按下述顺序分析属性。例如，如果对于用户身份验证，身份是 userA@example.com（其中 username=userA 且 domain=example.com），对于计算机身份验证，身份是 hostA.example.com（其中 username=hostA 且 domain=example.com），将分析以下属性：
- 如果是基于用户证书的身份验证：
  - SubjectAlternativeName: UPN = userA@example.com
  - Subject = .../CN=userA@example.com/...
  - Subject = userA@eample.com
  - Subject = .../CN=userA/DC=example/DC=com/...
  - Subject = userA (no domain)
- 如果是基于计算机证书的身份验证：
  - SubjectAlternativeName: DNS = hostA.example.com
  - Subject = .../DC=hostA.example.com/...
  - Subject = .../CN=hostA.example.com/...
  - Subject = hostA.example.com
- 如果凭证源是最终用户 - 从用户输入的信息获取占位符的值。
- 如果从操作系统获取证书 - 从登录信息获取占位符的值。
- 如果凭证是静态的 - 没有使用占位符。

在 Credentials 窗格中，您可以指定用于对关联网络进行身份验证所需的凭证。

步骤 1 定义受保护身份模式的用户身份。网络访问管理器支持以下身份占位符模式：

- [username] - 指定用户名。如果用户输入 username@domain 或 domain\username，则域部分会被剥离。

- [raw] - 完全按照用户的输入指定用户名。
- [domain] - 指定用户设备的域。

步骤 2 指定典型的未受保护的身份模式。

尚未协商的会话遇到身份请求，并以明文响应，而无需完整性保护或身份验证。这些会话可能遭到监听和数据包修改。

- anonymous@[domain] - 常常用在隧道方法中，用于在以明文发送值时隐藏用户身份。在内部方法中，将真实用户身份提供为受保护的身份。
- [username]@[domain] - 用于非隧道化方法。

  注释 以明文发送未受保护的身份信息。如果初始明文身份请求或响应被篡改，服务器可能会发现一旦建立了 TLS 会话就无法验证身份。例如，用户 ID 可能无效或不在 EAP 服务器处理的领域内。

步骤 3 指定保护身份模式。

为防止用户 ID 被监听，明文身份只能提供足以让身份验证请求路由到正确领域的信息。

- [username]@[domain]
- 用作用户身份的实际字符串（无占位符）

步骤 4 提供更多用户凭证信息：

- Use Single Sign On Credentials - 从操作系统的登录信息中获取凭证。如果登录凭证失败，网络访问管理器暂时（直到下次登录）开启并提示用户通过 GUI 提供凭证。

  注释 您不能将 Windows 登录凭证与网络访问管理器和 SSO 一起自动使用。将 SSO 与网络访问管理器一起使用需要拦截登录凭证；因此，系统将在安装或注销后提示您重新启动。

- Use Static Credentials - 从该配置文件编辑器提供的网络配置文件获取用户凭证。如果静态凭证失败，网络访问管理器在加载新配置之后才会再次使用凭证。

  注释 在此字段中，& 符号是无效字符。

- Prompt for Credentials - 通过 AnyConnect GUI 获取来自最终用户的凭证，正如下文所指定：
  - Remember Forever - 永久记住凭证。如果记住的凭证失败，则再次提示用户输入凭证。凭证保留在文件中，并使用本地计算机密码进行加密。
  - Remember While User Is Logged On - 记住凭证，直到用户注销为止。如果记住的凭证失败，则再次提示用户输入凭证。
  - Never Remember - 从不记住凭证。网络访问管理器每次需要凭证信息以进行身份验证时都会提示用户。

步骤 5 在需要证书时确定哪个证书源用于进行身份验证：

- 智能卡或操作系统证书 - 网络访问管理器使用在操作系统证书存储库或智能卡中找到的证书。

- 仅限智能卡证书 - 网络访问管理器仅使用智能卡中找到的证书。

步骤 6 在 Remember Smart Card Pin 参数中，确定网络访问管理器记住用于从智能卡检索证书的 PIN 的时间长度。请参阅步骤 2 以了解可用的选项。

注释 PIN 保留时间绝不能超过证书本身的保留时间。

某些智能卡连接所需时间可能比其他智能卡更长，这取决于智能卡芯片和驱动程序（也称为加密服务提供程序 (CSP) 和密钥存储提供程序 (KSP)）。增加连接超时可能给网络足够时间来执行基于智能卡的身份验证。

配置计算机凭证

EAP 对话可能涉及多种 EAP 身份验证方法，其中每种身份验证要求的身份可能不同（例如先是计算机身份验证，然后是用户身份验证）。例如，对等成员最初可能要求 nouser@example.com 的身份来将身份验证请求路由到 cisco.com EAP 服务器。但是，一旦 TLS 会话经过协商，对等成员就可能要求 johndoe@example.com 的身份。因此，即使通过用户的身份提供保护，目标领域也不一定匹配，除非对话在本地身份验证服务器上终止。

对于计算机连接，只要使用 [username] 和 [domain] 占位符，以下条件即适用：

- 如果客户端证书用于身份验证 - 从各 X509 证书属性获取 [username] 和 [password] 的占位符值。根据首次匹配按下述顺序分析属性。例如，如果对于用户身份验证来说身份是 userA@cisco.com（其中 username=userA，domain=cisco.com），对于计算机身份验证来说是 hostA.cisco.com（其中 username=hostA，domain=cisco.com），则分析以下属性：
- 如果是基于用户证书的身份验证：
  - SubjectAlternativeName: UPN = userA@example.com
  - Subject = .../CN=userA@example.com/...
  - Subject = userA@example.com
  - Subject = .../CN=userA/DC=example.com/...
  - Subject = userA (no domain)
- 如果是基于计算机证书的身份验证：
  - SubjectAlternativeName: DNS = hostA.example.com
  - Subject = .../DC=hostA.example.com/...
  - Subject = .../CN=hostA.example.com/...
  - Subject = hostA.example.com
- 如果客户端证书不用于身份验证 - 从操作系统获取凭证，[username] 占位符代表分配的计算机名称。

使用凭证面板，可以指定所需的计算机凭证。

步骤 1 为受保护的身份模式定义计算机身份。网络访问管理器支持以下身份占位符模式：

- [username] - 指定用户名。如果用户输入 username@domain 或 domain\username，则会删除域部分。
- [raw] - 完全按照用户的输入指定用户名。
- [domain] - 指定用户 PC 的域。

步骤 2 定义典型的未受保护的计算机身份模式。

尚未协商的会话遇到身份请求，并以明文响应，而无需完整性保护或身份验证。这些会话可能遭到监听和数据包修改。

- host/anonymous@[domain]
- 作为计算机身份发送的实际字符串（无占位符）

步骤 3 定义受保护的计算机身份模式。

为防止用户 ID 被监听，明文身份只能提供足以让身份验证请求路由到正确领域的信息。典型的受保护的计算机身份模式如下所示：

- host/[username]@[domain]
- 作为计算机身份使用的实际字符串（无占位符）

步骤 4 提供更多计算机凭证信息。

- 使用机器凭证 - 从操作系统获取凭证。
- 使用静态凭证 - 指定要在部署文件中发送的实际静态密码。静态凭证不适用于基于证书的身份验证。

设置网络访问管理器以选择正确的证书

在客户端身份验证时，如果有两个证书，则网络访问管理器将根据证书属性自动选择最佳证书。由于首选证书的条件因客户而已，所以您必须配置以下字段来确定证书选择，并提供需要的规则来覆盖证书选择。

如果多个证书与同一个规则匹配或者没有证书与规则匹配，则ACE引擎将根据算法对证书优先级进行排序，并根据特定条件（例如，是否有私钥，是否来自设备存储库等）选择一个证书。如果多个证书具有相同的优先级，ACE 引擎将选择在该优先级中找到的第一个证书。

步骤 1 从 AnyConnect 配置文件编辑器中，选择“**网络**”**(Networks)** 选项卡。

步骤 2 选择要编辑的网络。

步骤 3 选择**计算机凭证 (Machine Credentials)** 选项卡。

步骤 4 在页面底部，选择**使用证书匹配规则 (Use Certificate Matching Rule)**。

步骤 5 从“证书字段”(Certificate Field) 下拉菜单中，选择您要的搜索条件。

步骤 6 从“匹配”(Match) 下拉菜单中，确定搜索是否包含字段完全匹配（等于）或字段部分匹配（包括）。

步骤 7 在“数值”(Value) 字段中，输入证书搜索条件。

配置受信任服务器验证规则

为 EAP 方法配置了“验证服务器身份”(Validate Server Identity) 选项时，“证书”(Certificate) 面板允许您配置证书服务器或授权的验证规则。验证的结果将确定证书服务器或授权是否得到信任。

要定义证书服务器验证规则，请执行以下步骤：

步骤 1 显示**证书字段 (Certificate Field)** 和**匹配 (Match)** 列的可选设置时，单击下拉箭头并选择所需的设置。

步骤 2 在 Value 字段中输入值。

步骤 3 在“规则”(Rule) 下，单击**添加 (Add)**。

步骤 4 在“受信任证书颁发机构”(Certificate Trusted Authority) 窗格中，选择以下选项之一：

- 信任安装在操作系统上的所有根证书颁发机构 (CA) (Trust Any Root Certificate Authority [CA] Installed on the OS) - 如果选择此选项，仅将本地计算机或证书存储区视为服务器的证书链验证。
- 包括根证书颁发机构 (CA) 证书。

  注释 如果选择“包括根证书颁发机构 (CA) 证书”(Include Root Certificate Authority [CA] Certificates)，则必须单击**添加 (Add)** 将 CA 证书导入到配置。如果使用的证书正在从 Windows 证书库中导出，请使用“Base 64 encoded X.509 (.cer)”选项。

Network Groups 窗口

在 Network Groups 窗口中，可向特定的组分配网络连接。对连接分组提供多项优势：

- 当用户尝试连接时，可改善用户体验。当配置了多个隐藏网络时，客户端可以按照定义的顺序遍历隐藏网络列表，直到成功建立连接。在这些情况下，分组可大幅减少建立连接所需的时间。
- 简化所配置连接的管理。使您可以根据需要将管理员网络与用户网络分隔，并允许公司的多角色用户（或经常访问同一区域的用户）在组中定制网络，以提高可选网络列表的可管理性。

作为分发包的一部分而定义的网络将锁定，从而防止用户编辑配置设置或删除网络配置文件。

您可以将网络定义为全局网络。执行此操作时，网络将显示在全局网络部分中。该部分划分为有线和无线网络类型。在这种类型的网络中只能执行排序编辑。

所有非全局网络必须存在于一个组中。默认情况下，会创建一个组，如果所有网络都是全局网络，用户可以删除该组。

步骤 1 从下拉列表选择一个组。

步骤 2 选择**创建网络 (Create networks)** 可允许最终用户在该组中创建网络。部署后，如果您取消选中此项，网络访问管理器会从该组中删除用户创建的任何网络，这会强制用户在另一个组中重新输入网络配置。

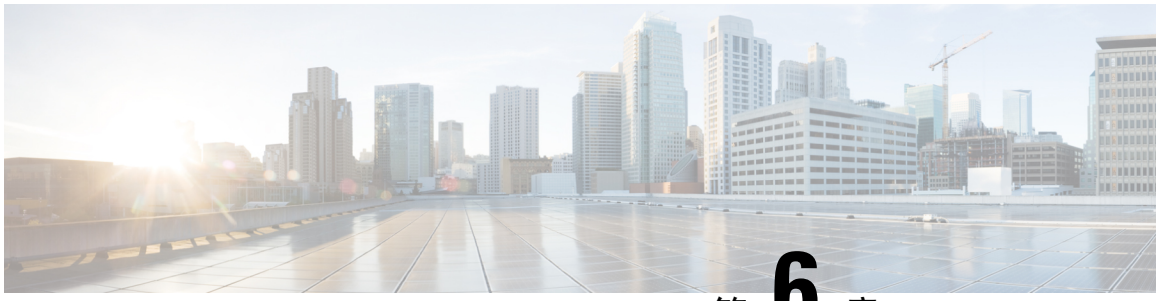
步骤 3 选择**查看扫描列表 (See scan list)**，以在使用 AnyConnect GUI 将该组选择为活动组时允许最终用户查看扫描列表。或者，清除复选框以限制用户查看扫描列表。例如，如果您要阻止用户意外连接到相邻设备，应限制扫描列表访问。

注释 这些设置应用基于组。

步骤 4 使用右箭头和左箭头从在“组”(Group) 下拉列表中选择的组中插入和删除网络。如果某网络已移出当前组，则它会放置到默认组中。当默认组正在编辑时，您无法从其中移动网络（使用 > 按钮）。

注释 在给定网络中，每个网络的显示名称必须唯一。因此，任何一组不能包含两个或更多具有相同显示名称的网络。

步骤 5 使用上箭头和下箭头更改组中网络的优先级顺序。



第 6 章

配置终端安全评估

AnyConnect 安全移动客户端提供 VPN 终端安全评估 (HostScan) 模块和 ISE 终端安全评估模块。这两个模块都为Cisco AnyConnect Secure Mobility Client提供了评估终端在以下方面是否合规的功能，例如主机上所安装的防病毒、反间谍软件以及防火墙软件。您可以限制网络访问权限直至终端合规，或者提高本地用户的权限，使其可以制定补救措施。

VPN 终端安全评估与 hostscan_version.pkg 捆绑在一起，后者是一款收集主机上安装了哪些操作系统、防病毒软件、反间谍软件和其他软件的应用。ISE 终端安全评估可在访问 ISE 控制的网络时部署一个客户端，而不必部署 AnyConnect 和 NAC 代理。ISE 终端安全评估是一个模块，可选作额外的安全组件安装到 AnyConnect 产品中。HostScan 包含在 AnyConnect 捆绑包版本 3.x 中，但现在需要单独安装。

ISE 终端安全评估可执行客户端评估。客户端从头端获得终端安全评估要求策略、执行终端安全评估数据收集、将结果与策略进行比较，并将评估结果发送回头端。尽管ISE实际确定终端是否合规，但它依赖终端自己的策略评估结果。

相反，HostScan 将执行服务器端评估，其中 ASA 仅请求终端属性（例如操作系统、IP 地址、注册表项、本地证书和文件名）的列表，而且这些属性由 HostScan 返回。根据策略评估的结果，您可以控制哪些主机可获准与安全设备建立远程访问连接。

注释 不支持组合使用 HostScan 和 ISE 终端安全评估代理。运行两个不同的终端安全评估代理时会出现意外结果。

HostScan 中支持以下终端安全评估检查，但不支持 ISE 终端安全评估：主机名、IP 地址、MAC 地址、端口号、OPSWAT 版本、BIOS 序列号和证书字段属性。

ISE 终端安全评估模块提供的功能

终端安全评估检查

ISE 终端安全评估模块使用 OPSWAT 版本 3 或版本 4 的库来执行终端安全评估检查。对于初始终端安全评估检查，任何未能满足所有强制性要求的终端都被视为不合规。其他终端授权状态为终端安全评估未知或合规（满足强制性要求）。

注释 对于 macOS 64 位迁移，AnyConnect 4.6 ISE 终端安全评估模块与旧的 OPSWAT v3 合规性模块不兼容。

如果在终端安全评估检查阶段出错并且 AnyConnect 能够继续，用户将收到通知，但如果可能，终端安全评估检查将继续。如果在强制终端安全评估检查期间出错，检查将标记为失败。如果满足所有强制性要求，将授予网络访问权限。否则，用户可以重新启动终端安全评估进程。

任何必要的补救措施

补救窗口在后台运行，以保证网络活动更新不会弹出，引起干扰或中断。您可以在 AnyConnect UI 的 ISE 终端安全评估图块部分单击**详细信息 (Details)**，查看检测到的内容和您加入网络前所需的更新。如果必须进行手动补救，补救窗口会打开，显示需要操作的项目。此“系统扫描”窗口显示更新的进度、所分配更新时间的剩余时间、任何要求的状态以及系统合规性状态。

注释 需要提升权限的应用仅使用非管理员用户帐户进行自动补救。管理员帐户必须手动执行补救。

注释 仅在服务器受信任时才会执行需要更高权限的终端安全评估检查和补救。

当仅剩下可选更新时，才可选择**跳过 (Skip)** 跳到下一步操作，或选择**全部跳过 (Skip All)** 以忽略所有剩余补救项。您可以出于时间考虑跳过可选补救项或仍然保持网络访问。

在补救后（或在无需补救时执行要求检查后），您可能收到可接受使用策略的通知。它要求您接受该策略才能进行网络访问，若拒绝则限制访问。在此部分补救过程中，AnyConnect UI 的终端安全评估图块部分会显示 System Scan: Network Acceptable Use Policy。

当补救完成后，作为所需更新列出的所有检查都显示 Done 状态和绿色复选框。补救后，代理会向 ISE 发送终端安全评估结果。

补丁管理检查和补救

AnyConnect 4.x 和 Microsoft 系统中心配置管理器 (SCCM) 集成提供了补丁管理检查和补丁管理补救。它将检查终端上缺失的重要补丁的状态，以查看是否应该触发软件补丁。如果 Windows 终端上没有缺失重要补丁，则补丁管理检查将通过。补丁管理补救只会为管理员级用户触发，并且仅当 Windows 终端上缺失一个或多个重要补丁时才会触发。

如果 SCCM 客户端安装的某个补丁是在重新启动之前安装的，则 SCCM 客户端将在计算机重新启动后尽快报告该补丁的安装状态（已安装或未安装）。但是，如果 SCCM 客户端安装的某个补丁是在重新启动之后开始安装的，则 SCCM 客户端不会立即报告该补丁的状态。

AnyConnect 合规性模块无法强制 SCCM 客户端在此时提供任何状态。终端安全评估模块客户端完成本机 API 请求所花费的时间是不同动态 OS 参数（例如 CPU 负载、挂起修补程序数量、修补程序安装后无重启等）以及网络因素（如终端安全评估模块客户端和服务器之间的连接和延迟）的函数。您可能必须等待 SCCM 客户端响应，但对已知修补程序进行实验后，有些结果约为 10 分钟。

通过 Windows Server 更新服务 (WSUS) 搜索 API 也可观察到类似行为，它需要更多时间才会响应，有时长达 20 - 30 分钟。Windows 更新会检查所有 Microsoft 产品（例如 Microsoft Office）未安装的补丁，而不仅限于 Windows 操作系统。

请参阅策略条件了解如何在 ISE 上设置策略条件，或请参阅补丁管理补救了解有关补丁管理补救的更多信息。

重新评估终端合规性

当终端被视为合规并授予网络访问权限后，可选择基于管理员配置的控制对终端定期进行重新评估。被动重新评估终端安全评估检查与初始终端安全评估检查不同。如果管理员配置了相应的设置，那么当发生任何不符合要求的情形时，用户都可选择修复选项。配置设置用于控制用户是否维持受信任的网络访问（即使用户未达到一项或多项强制要求）。在初始终端安全评估过程中，如果终端未满足所有强制要求，将被视为不合规。默认情况下，此功能被禁用。如果为某一用户角色启用该功能，则每 1 到 24 小时执行一次终端安全重新评估。

管理员可将结果设置为“继续”(Continue)、“注销”(Logoff) 或“补救”(Remediate)，并可配置诸如强制执行和正常时间等其他选项。

您可以使用 ISE UI 创建在 AnyConnect 终端安全评估配置文件中显示的更多信息性消息。按钮文本和链接也可以自定义。

不兼容设备的宽限期

您可以在 Cisco ISE UI 中设置宽限期。通过此配置，可以向不符合要求、但在先前终端安全评估状态下符合要求的终端授予网络的访问权限。思科 ISE 在其缓存中查找先前已知的良好状态，并为设备提供宽限期。当宽限期到期时，AnyConnect 将再次执行终端安全评估检查（这一次不进行修复），并根据检查结果确定终端状态是否合规。

注释 当设备处于宽限期但在终端安全评估策略中更新时，会出现以下情况：

- （如果宽限期延长），在以前的宽限期过期或设备从 ISE 中删除时，系统将应用新的宽限期。
- （如果宽限期缩短），仅当设备再次经过终端安全评估流过程时，新的宽限期才会应用到设备。

宽限期不适用于临时代理、硬件库存和应用监控。

当用户处于宽限期时，定期重新评估 (PRA) 不适用。

当设备匹配多个终端安全评估策略（每个策略有不同的宽限期）时，设备将获取在不同策略中配置的最大宽限期。

将设备移至宽限期时，不会显示“可接受使用策略”(AUP)。

宽限期在 ISE UI 的**策略 > 终端安全状态或工作中心 > 终端安全状态 > 终端安全状态策略**中的 AnyConnect 终端安全评估下进行设置。有效值以天、小时或分钟为单位指定。默认情况下，此设置处于禁用状态。

灵活的通知

您可以使用“延迟通知”(Delay Notification) 选项来延迟自定义通知窗口的显示，直到经过特定百分比的宽限期。例如，如果 ISE UI 上的“延迟通知”字段设置为 50% 且配置的宽限期为 10 分钟，则 AnyConnect ISE 终端安全评估将在 5 分钟后重新扫描终端，并在发现终端不合规时显示通知窗口。如果终端状态为合规，则不会显示通知窗口。如果通知延迟时间设置为 0%，系统会在宽限期开始时立即提示用户以解决问题。在宽限期过期之前，终端会被授予访问权限。

如果终端不合规，只有在 ISE UI 上配置自定义通知时，AnyConnect UI 才会弹出警告。通知还指示宽限期的开始以及宽限期开始后不合规的任何终端。AnyConnect 系统扫描图块会突出显示所有终端安全评估失败，您可以单击**再次扫描 (Scan Again)** 按钮，以通过强制重新运行终端安全评估策略来维持完整的网络访问。

注释 若要显示“再次扫描”(Scan Again) 选项，必须将“启用重新扫描按钮”(Enable Rescan Button) 选项设置为“启用”(Enabled)。

在补救流程中，解决问题之前您基本上无法访问。没有可用的临时访问权限。在宽限期流程中，您可以获得延迟的访问权限，为您提供解决问题的宽限期。如果单击灵活通知流中的**启动浏览器 (Launch Browser)** 选项，则可以启动浏览器（如果服务器受信任）。您可以通过浏览器选项获取有关遵守终端安全评估策略的其他详细信息。

思科临时代理

思科临时代理专为 Windows 或 macOS 环境而设计，用于在用户接入受信任网络时共享合规性状态。思科临时代理在 ISE UI 中进行配置。每当思科临时代理尝试访问互联网时，系统便会将其可提取文件 .exe（适用于 Windows）或 dmg（适用于 macOS）下载到终端。用户必须运行下载的可执行文件或 dmg 以执行合规性检查：无需管理员权限。

然后，UI 会自动启动并开始检查，以确定终端是否合规。在完成合规性检查后，根据策略在 ISE UI 上的配置方式，ISE 可以采取任何必要的操作。

在 Windows 中，可执行文件为自提取文件，所有必要的 dll 和用于合规性检测的其他文件会被置于此提取文件的临时文件夹中。完成合规性检查后，系统会删除所有提取的文件和可执行文件。为了完全删除这些文件和可执行文件，用户必须退出 UI。

有关在 ISE UI 上执行配置的详细步骤，请参阅《思科身份服务引擎管理员指南，版本 *2.3*》中的思科临时代理工作流程。

思科临时代理的限制

- macOS 不支持临时代理的 VLAN 控制终端安全评估环境，因为在没有根权限的情况下无法执行刷新适配器（DHCP 续订）进程。临时代理可以仅作为用户进程运行。支持 ACL 控制的终端安全评估环境，因为它不需要刷新终端的 IP。
- 如果网络接口在补救期间发生，则用户必须离开当前 UI 并重新执行整个程序。
- 在 macOS 中，不会删除 dmg 文件。
- 在启动临时代理安装程序后，该安装程序在终端上运行时可能会隐藏在浏览器后面。要继续收集临时代理应用的运行状况，最终用户应将浏览器最小化。大部分 Windows 10 用户都会遇到该问题，因为在这些客户端上 UAC 模式设置为高，以接受以高安全条件运行的第三方应用。
- 在终端上启用隐藏模式时，无法使用临时代理。
- 思科临时代理不支持下列条件：
  - Service Condition-macOS - 系统后台守护程序检查
  - Service Condition-macOS - 后台守护程序或用户代理检查
  - PM - 最新检查
  - PM - 已启用检查
  - DE - 基于加密位置的检查

用于可选模式的终端安全评估策略增强功能

无论强制检查通过还是失败，均可在可选模式下对失败的要求检查执行补救。将在 AnyConnect ISE 终端安全评估 UI 上显示一条关于补救的消息，您可以查看哪些要求失败，哪些要求需要补救操作。

- Manual Remediation of Optional Mode - System Scan Summary 屏幕显示如果某种情况失败，可能需要补救的任何可选模式状态。您可以手动单击“开始”(Start) 进行补救，或者单击“跳过”(Skip)。即使补救失败，终端仍会符合要求，因为这些只是可选要求。System Summary 将显示它们是被跳过、已失败，还是已成功。
- Automatic Remediation of Optional Mode - 您可以监控 System Scan 图块，因为它会在应用可选更新时显示提示。不会要求您启动补救，因为补救是自动进行的。如果任何自动补救失败，您将收到一条消息，指出未能尝试补救。此外，如果需要，您还可以选择跳过补救操作。

查看硬件清单

ISE UI 的“上下文可见性”(Context Visibility) 下已添加了“终端”(Endpoints) > “硬件”(Hardware) 选项卡。它可以帮助您收集、分析和报告短时间内的终端硬件信息。您可以收集信息，例如查找内存容量低的终端或查找终端的 BIOS 型号/版本。根据查找结果，您可以增加内存容量，升级 BIOS 版本或在计划购买资产之前评估需求。制造商使用情况 Dashlet 显示运行 Windows 或 macOS 的终端的硬件清单详细信息，终端使用情况 Dashlet 显示终端的 CPU、内存和磁盘利用率。有关详细信息，请参阅《思科身份服务引擎管理员指南，版本 2.3》的“硬件”(Hardware) 选项卡。

隐身型号

管理员可在从终端用户客户端隐藏 AnyConnect UI 图块时配置 ISE 终端安全评估。不会显示任何弹出消息，并且任何需要用户干预的情形都将采取默认操作。此功能可在 Windows 和 macOS 操作系统上使用。

请参阅思科身份服务引擎管理员指南中的配置终端安全评估策略部分，您可以在此处将无客户端状态下的隐身型号指定为禁用或启用。

在 ISE 用户界面上，您可以将隐身型号设置为启用通知，以便最终用户仍然看到错误通知。

在映射 ISE 终端安全评估配置文件编辑器，第 205 页中的配置文件，然后将 AnyConnect 配置映射到 ISE 中的 Client Provisioning 页面后，AnyConnect 即可读取终端安全评估配置文件，将其设置为预期型号，以及在初始终端安全评估请求期间将与选定型号相关的信息发送到 ISE。根据型号和其他因素（如身份组、OS 及合规性模块），思科 ISE 将与适当政策进行匹配。

请参阅思科身份服务引擎管理员指南中的隐身型号部署及其影响。

ISE 终端安全评估不允许您在隐身型号下设置以下功能：

- 任何手动补救
- 链接补救
- 文件补救
- WSUS 显示 UI 补救
- 激活 GUI 补救
- AUP 策略

终端安全评估策略实施

要提高您的终端上安装的软件的整体可见性，我们提供了以下终端安全评估增强功能：

- 您可以检查终端防火墙产品的状态，以查看其是否正在运行。如果需要，可以启用防火墙，并在首次终端安全评估和定期重新评估 (PRA) 过程中实施策略。要设置，请参阅思科身份服务引擎配置指南中的防火墙条件设置部分。

- 同样，您可以对终端上安装的应用运行查询。如果运行或安装了不需要的应用，则可停止该应用，或者卸载不需要的应用。要设置，请参阅思科身份服务引擎配置指南中的应用补救部分。

UDID 集成

在设备上安装 AnyConnect 时，它会在 AnyConnect 中的所有模块中共享自己的唯一标识符 (UDID)。此 UDID 是终端的标识符，并将另存为终端属性，这可确保对特定终端而非 MAC 地址的终端安全评估控制。随后您可基于该 UDID 查询终端，它是一个常量，无论该终端如何连接，甚至是在更新或卸载后也不会改变。随后，ISE UI **(Context Visibility > Endpoints > Compliance)** 上的 Context Visibility 页面可为装有多个 NIC 的中断显示一个条目（而非多个条目）。

应用监控

终端安全评估客户端可以持续监控不同终端属性，以便观察动态变化，并向策略服务器汇报。根据终端安全评估的配置，您可以监控不同属性，如安装和运行了哪些应用用于反间谍软件、防病毒、防恶意软件、防火墙等。有关应用条件设置的详细信息，请参阅思科身份服务引擎管理员指南中的持续终端属性监控部分。

USB 存储设备检测

在将 USB 大容量存储设备连接到 Windows 终端时，终端安全评估客户端可以检测到该设备，并将根据终端安全评估策略块阻止或允许该设备。通过 USB 检测，只要终端仍然位于同一个受 ISE 控制的网络中，代理即可持续监控该终端。如果在此时段内连接了符合该条件的 USB 设备，将执行指定的补救操作。还会向策略服务器报告该事件。

USB 存储检测需要依靠 OPSWAT v4 合规性模块。必须在 ISE UI 上的定期重新评估策略 (PRA) 中配置 USB 检查，位于 **Work Centers > Posture > Policy Elements > USB**。

注释 将按顺序执行检查和补救，因此将其他检查的 PRA 宽限期设定为最小值可以防止处理 USB 检查时的延迟。宽限期在 ISE UI 上的 **Work Centers > Posture > Settings > Reassessment Config** 中进行设置。

有关在 ISE UI 上配置 USB 存储设备检测的步骤，请参阅 USB 大容量存储设备检查工作流程。

自动合规性

凭借终端安全评估租约，ISE 服务器可以完全跳过终端安全评估检查，直接将系统置于合规状态。通过此功能，如果最近检查过系统终端安全评估，用户不必再经历网络间切换的延迟。ISE 终端安全评估代理仅需在发现 ISE 服务器后立即向 UI 发送状态消息，指示系统是否合规。在 ISE UI（“设置”(Settings)>“终端安全评估”(Posture)>“常规设置”(General Settings)）中，您可以指定在初始合规性检查后多长时间内，将终端视为满足安全评估要求。即使用户从一个通信接口切换到另一个，也应保持合规状态。

注释 使用终端安全评估租约时，如果 ISE 上的会话有效，终端会从未知状态变为合规状态。

VLAN 监控和转换

某些站点使用不同的 VLAN 或子网划分其集团公司和访问级别的网络。来自 ISE 的授权更改 (CoA) 指定VLAN更改。管理员操作（例如会话终止）也可能导致发生更改。为支持有线连接期间的VLAN更改，请在 ISE 终端安全评估配置文件中配置以下设置：

- VLAN Detection Interval - 确定代理检测 VLAN 转换的频率以及监控是否禁用。当此时间间隔设置为非 0 值时，会启用 VLAN 监控。对于 macOS，将此值至少设置为 5。

  VLAN 监控在 Windows 和 macOS 上都可实施，但在 macOS 上仅当检测意外 VLAN 更改时才需要实施。如果 VPN 已连接或者 acise（主要 AnyConnect ISE 进程）未运行，它会自动禁用。有效范围为 0 到 900 秒。

- 启用代理 IP 地址刷新 (Enable agent IP refresh) - 未选中时，ISE 会向代理发送“网络过渡延迟”(Network Transition Delay) 值。选中后，ISE 将向代理发送 DHCP 释放和续订值，然后代理更新 IP 以检索最新的 IP 地址。

- DHCP Release Delay and DHCP Renew Delay - 用于关联 IP 刷新和 Enable Agent IP Refresh 设置。选中“启用代理 IP 地址刷新” (Enable agent IP refresh) 复选框且此值不是 0 时，代理会等待一定秒数的释放延迟，更新 IP 地址，然后等待一定秒数的续订延迟。如果 VPN 已连接，将自动禁用 IP 刷新。如果 4 次连续探测被丢弃，将会触发 DHCP 刷新。
- 网络过渡延迟 (Network Transition Delay) - 当 VLAN 监控被代理禁用或启用（在 Enable Agent IP Refresh复选框中）时使用。此延迟在未使用VLAN时会增加缓冲，给代理适当的时间等待来自服务器的准确状态。ISE 将此值发送给代理。如果您还在 ISE 用户界面的全局设置中设置了 Network Transition Delay 值，ISE 终端安全评估配置文件编辑器中的值将覆盖它。

注释 ASA 不支持 VLAN 更改，因此这些设置在客户端通过 ASA 连接到 ISE 时不适用。

故障排除

如果终端设备在终端安全评估完成后无法访问网络，请检查以下内容：

- 在 ISE 用户界面上是否配置了 VLAN 更改？
  - 如已配置，是否在配置文件中设置了 DHCP 释放延迟和续订延迟？
  - 如果这两项设置都为 0，是否在配置文件中设置了 Network Transition Delay？

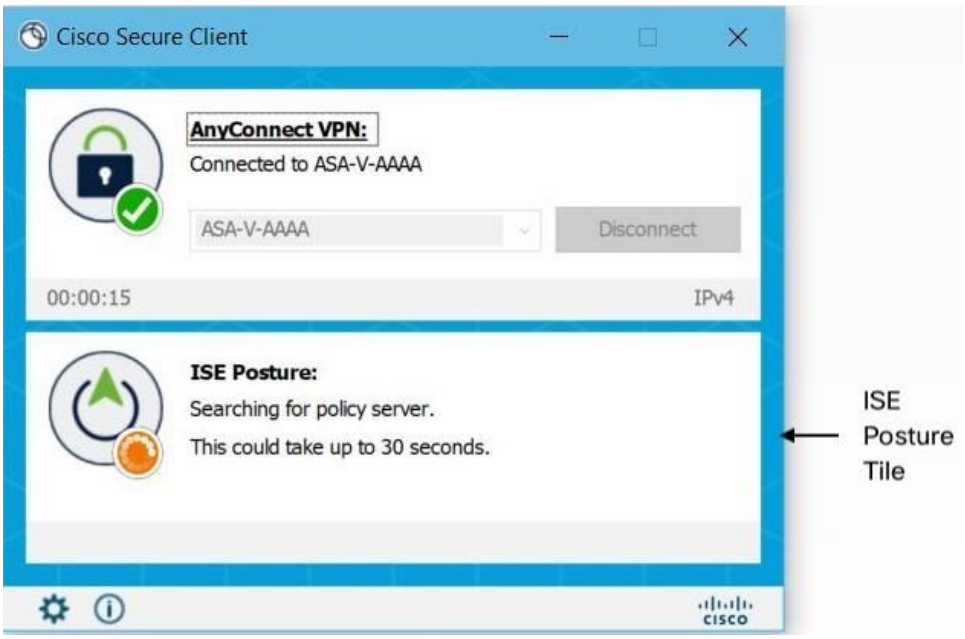
用于中断 AnyConnect ISE 流的操作

由于各种原因，在初始终端安全评估重新评估或被动重新评估过程中，AnyConnect ISE 终端安全评估流可能中断。

- 用户取消 AnyConnect ISE - 在终端安全评估检查和补救期间，用户可以取消 AnyConnect ISE。UI 会立即通知用户正在进行取消，但只在避免将终端置于出问题状态的时期才会出现这种情况。如果使用了第三方软件，一些取消操作可能需要重新启动。取消后，AnyConnect UI 的终端安全评估图块部分显示合规状态。
- 修复计时器超时 - 满足终端安全评估要求的管理员控制时间已到期。一份评估报告被发送到前端。在被动重新评估期间，用户保留网络访问权限。而对于终端安全评估，满足所有强制性要求后将授予网络访问权限。
- 终端安全评估检查过程中出错 - 如果在终端安全评估检查阶段出错并且 AnyConnect 能够继续，用户将收到通知，但如果可能，终端安全评估检查将继续。如果在强制终端安全评估检查期间出错，检查将标记为失败。如果满足所有强制性要求，将授予网络访问权限。否则，用户可以重新启动终端安全评估进程。
- 补救过程中出错 - 如果在补救阶段出错并且 AnyConnect ISE 终端安全评估可以继续，用户会收到通知。如果失败的补救步骤与某个强制性终端安全评估要求相关，AnyConnect ISE 终端安全评估将停止补救进程。如果失败的补救步骤与某个可选终端安全评估要求相关，则会尝试继续下一步并完成 ISE 终端安全评估操作。如果满足所有强制性要求，将授予网络访问权限。否则，用户可以重新启动终端安全评估进程。
- 默认网关更改 - 用户可能由于默认网关更改而失去受信任网络访问，导致 ISE 终端安全评估尝试重新发现 ISE。当 ISE 终端安全评估进入重新发现模式时，AnyConnect UI 的 ISE 终端安全评估图块部分会显示 ISE 终端安全评估的状态。
- AnyConnect 和 ISE 之间的连接丢失 - 终端被认为合规并被授予网络访问权限后，可能发生各种网络状况：终端可能遇到网络连接完全丢失的情况，ISE 可能性能下降，ISE 终端安全评估可能出现故障（由于会话超时、手动重启等）或 ASA 后面的 ISE 可能丢失 VPN 隧道。
- 使用 ISE 终端安全评估时，不能在 macOS 终端上登录多个控制台用户。
- 初始化和终端安全评估流程延迟（仅 macOS）- Apple 建议您允许其子网处于终端安全评估前阶段，以避免合规性模块库签名验证失败。

ISE 终端安全评估的状态

当 AnyConnect ISE 终端安全评估按预期正常运行和阻止网络访问时，AnyConnect 用户界面的 ISE 终端安全评估图块中显示“System Scan: Searching for policy server”。在 Windows 任务管理器或 macOS 系统日志中，您可以看到该进程正在运行。如果该服务未运行，AnyConnect 用户界面的 ISE 终端安全评估图块中显示“System Scan: Service is unavailable”。



网络变化启动发现阶段。使用 AnyConnect ISE 终端安全评估时，如果主要接口的默认路由发生更改，会使代理回到发现过程。例如，当 WiFi 和主要 LAN 连接时，代理会重新启动发现。同样，如果 WiFi 和主要 LAN 建立连接，然后 WiFi 断开连接，则代理不会重新启动发现。

在 AnyConnect 用户界面的 ISE 终端安全评估图块中的“System Scan”之后，还可能出现以下状态消息：

- Limited or no connectivity - 未进行发现，因为您没有连接。AnyConnect ISE 终端安全评估代理可能正在网络中的错误终端上执行发现。
- System scan not required on current WiFi - 未进行发现，因为检测到不安全的 WiFi。AnyConnect ISE 终端安全评估代理仅在 LAN、无线网络（如果使用 802.1X 身份验证）以及 VPN 上启动发现。WiFi 可能不安全，或者您通过在代理配置文件中将 OperateOnNonDot1XWireless 设置为 1 禁用了该功能。
- Unauthorized policy server - 主机与 ISE 网络的服务器名称规则不匹配，因此网络访问受限或不允许访问。
- The AnyConnect Downloader is performing update... - 下载程序已调用，将比较软件包版本、下载 AnyConnect 配置，并执行必要的升级。
- Scanning System... - 扫描防病毒和反间谍软件安全产品是否已启动。如果在此过程中网络发生更改，代理将循环生成日志文件的过程，并且状态返回到“No policy server detected”。
- Bypassing AnyConnect scan - 网络配置为使用思科 NAC 代理。
- “被用户取消的不受信任的策略服务器”(Untrusted Policy Server Cancelled by the user) - 在 AnyConnect 用户界面中使用“系统扫描首选项”(System Scan Preferences) 选项卡取消阻止连接到不受信任的服务器时，弹出窗口中会出现 AnyConnect 下载程序的安全警告。在此警告页面上单击**取消连接 (Cancel Connection)** 时，ISE 终端安全评估图块会更改为此状态。

- Network Acceptable Use Policy - 访问网络时，您必须查看并接受“可接受的使用策略”。拒绝该政策可能会导致网络访问受限。
- Updating Network Settings - 在 ISE 用户界面的 Settings > Posture > General Settings 中，您可以指定网络转换之间应发生的延迟秒数。
- Not Compliant. Update time expired - 为补救设置的时间已过期。
- Compliant. Network access allowed. - 补救完成。System Scan > Scan Summary 也显示状态为完成。
- No policy server detected - 找不到 ISE 网络。30 秒钟后，代理会减慢探测。默认网络访问权限生效。

脚本补救消息传送

您可能会在脚本补救过程中看到补救或用户通知弹出窗口，除非您是在用户界面有限的 Linux 中运行。要使脚本补救成功，指纹必须存在于 AnyConnectLocalPolicy.xml 中。您可能会遇到有关脚本补救的以下消息：

- **由于脚本包含无效散列，因此无法尝试补救 (Remediation cannot be attempted because the script has an invalid hash)** - 当下载的脚本存在散列不匹配或者策略签名验证失败时，会在系统扫描详细信息中显示此消息。
- **您尝试运行的脚本退出并出现错误 (The script you are trying to run exits with an error)** - 当脚本存在非零退出代码时，会在系统扫描详细信息中显示此消息。 在 Windows 中，配置的执行策略也可能不允许执行脚本。
- **补救由于脚本超时而不成功 (Remediation was unsuccessful because the script timed out)** - 当脚本花费的时间超出补救计时器的退出时间时，会在系统扫描详细信息中显示此消息。如果脚本未在剩余补救计时器的时间内退出，则 AnyConnect 会停止脚本并将补救标记为失败。
- **由于您连接到了不受信任的服务器，因此无法执行补救 (Remediation cannot be done because you are connected to an untrusted server)** - 当终端连接到不受信任的 ISE 服务器时，会在系统扫描详细信息中显示此消息。服务器证书在证书存储库中未被标记为受信任，或者您没有在 AnyConnectLocalPolicy.xml 中配置指纹。ISE 提供的证书中的指纹必须与 AnyConnectLocalPolicy.xml 中配置的指纹匹配。

终端安全评估和多宿主

AnyConnect ISE 终端安全评估模块不支持多宿主，因为此类场景的行为未定义。例如，当介质模式从有线更改为无线然后返回到有线时，即使终端实际上在有线连接上进行重定向，用户也可能会看到安全状态 ISE 终端安全评估模块的评估状态是合规的。

终端上的并发用户

当多名用户同时登录到终端而共享网络连接时，AnyConnect ISE 不支持单独的终端安全评估。当运行 AnyConnect ISE 的第一位用户的状态被成功捕获时，终端将被授予受信任的网络访问权限，该终端上的所有其他用户都将继承网络访问权限。为防止发生此情况，管理员可在终端上禁用允许并发用户的功能。

终端安全评估模块的日志记录

对于 ISE 终端安全评估，事件将写入本地操作系统的事件日志（Windows 事件日志查看器或 macOS 系统日志）。

对于 VPN 终端安全评估 (HostScan)，任何错误和警告都将写入系统日志（适用于非 Windows）和事件查看器（适用于 Windows）。所有可用的消息都将写入日志文件。

VPN 终端安全评估 (HostScan) 模块组件最多输出到三个日志，具体取决于您的操作系统、权限级别和启动机制（Web 启动或 AnyConnect）：

- cstub.log - 使用 AnyConnect Web 启动时捕获日志记录。
- libcsd.log - 由使用 VPN 终端安全评估 API 的 AnyConnect 线程创建。调试条目根据日志记录级别配置写入此日志。
- cscan.log - 通过扫描可执行文件 (cscan.exe) 而创建，是 VPN 终端安全评估的主要日志。调试条目根据日志记录级别配置写入此日志。

终端安全评估模块的日志文件和位置

对于 ISE 终端安全评估，事件包含在安装的 AnyConnect 版本的事件子文件夹中，因此易于与其余 AnyConnect 事件隔开。每个查看器均可搜索关键字和过滤。Web 代理事件写入标准应用日志。

为便于故障排除，会将 ISE 终端安全评估要求策略和评估报告记录到终端上经过模糊处理的单独文件中，而不会是事件日志中。某些日志文件的大小（例如 aciseposture），可由管理员在配置文件中配置。但 UI 日志大小是预定义的。

每当进程异常终止时，都会生成一个小型转储文件，就像其他 AnyConnect 模块提供的一样。

对于 VPN 终端安全评估 (HostScan)，文件位于以下目录下的用户主文件夹中：

- （非 Windows）- .cisco/hostscan/log
- (Windows) - C:\Users\<user_name>\AppData\Local\Cisco HostScan\log\cscan.log

ISE 终端安全评估配置文件编辑器

管理员可以选择使用独立编辑器创建终端安全评估配置文件，然后将其上载至 ISE。否则，嵌入式终端安全评估配置文件编辑器配置在 ISE 用户界面中的 Policy Elements 下。AnyConnect 配置编辑器在 ISE 中启动后，它会创建 AnyConnect 配置以及 AnyConnect 软件及其关联的模块、配置文件、OPSWAT 和任何定制。ASA 中 ISE 终端安全评估的独立配置文件编辑器包含以下参数：

- 代理的行为
  - **启用签名检查 (Enable signature check)** - 如果选中，则在代理运行可执行文件之前，会启用这些文件的签名检查。
  - **Log file size** - 代理日志文件的最大大小。有效值为 5 Mb 到 200 Mb。
  - **修复计时器** - 用户必须在此时间内完成修复，否则将被标记为不合规。有效值为 1 - 300 分钟。
  - **Enable agent log trace** - 在代理上启用调试日志。
  - **在非 802.1X 无线网络上运行 (Operate on non-802.1X wireless networks)** - 如果选中，会启用代理在非 802.1X 无线网络上工作。
  - **启用终端安全评估状态非重定向流 (Enable posture non-redirection flow)**- 如未选中，则会禁用终端安全评估状态非重定向流。在禁用之前，请确保所有 NAD 均支持重定向。
  - **启用隐身模式 (Enable Stealth Mode)** - 选择是否启用 隐身型号，这将允许终端安全评估作为服务运行，而无需用户干预。
  - **Enable Stealth With Notification** - 如果隐身型号通知设置为启用，则当 AnyConnect 隐身型号出现处于不合规状态、网络访问受限、有无法访问的服务器等情况时，最终用户仍然会收到通知消息。
  - **启用重新扫描按钮 (Enable Rescan Button)** - 如果要在发生故障后、手动修复后或终端安全评估陷入停滞状态等情况后重启终端安全评估（或发现），请启用此按钮，以便在系统扫描图块中显示 **再次扫描 (Scan Again)** 选项。您可以在 ISE 终端安全评估配置文件中显示或隐藏该选项。单击**再次扫描 (Scan Again)** 时，系统将启动发现，并启动整个终端安全评估流。

注释 仅当终端安全评估配置文件中的 EnableRescan 标记设置为 1 时，图块中才会显示“再次扫描”。如果设置为 0，则“再次扫描”(Scan Again) 按钮仅在其以前通常显示的条件下显示（在此选项之前）。

注释 如果在 ISE 端发生配置文件更改，则 AnyConnect 图块将在系统下一次启动发现时反映相关更改。

- **禁用 UAC 弹出窗口** - 确定在策略验证期间是否显示“Windows 用户帐户控制 (UAC)”弹出窗口。如果使用默认值（未选中），在进行连接时系统会继续提示最终用户获得管理员权限。如果启用，在策略验证期间，最终用户将看不到 Windows 用户帐户控制 (UAC) 提示。通过禁用 UAC 提示，AnyConnect 终端安全评估使用系统进程进行权限升级，而不是“以管理员身份运行”。在禁用UAC提示之前，在用户具有本地管理员权限的设备上验证您的终端安全评估策略。
- **Backoff Timer Limit** - 输入 AnyConnect 发送 ISE 发现探测所需的最长时间。由于探测会增加更多流量，因此您应选择不会造成您的网络中断的值。
- **定期探测间隔 (Periodic Probe Interval)** - 指定“补偿计时器限制 (Backoff Timer Limit)”过后的发现探测间隔。AnyConnect 会持续发送具有给定间隔的定期探测，直到找到有效的 ISE 服务器。默认值为 30 分钟，在初始几轮探测后，会持续以 30 分钟的间隔发送探测。将该值设置为 0 会禁用定期探测。

- **IP 地址更改**

  为了获得最佳用户体验，请将以下值设置为我们推荐的值。

  - **VLAN detection interval** - 代理在刷新客户端 IP 地址之前尝试检测 VLAN 更改的时间间隔。有效范围为 0 到 900 秒，推荐值为 5 秒。
  - **Ping or ARP** - 检测 IP 地址更改的方法。建议设置是 ARP，因为默认网关可以配置为阻止 ICMP 数据包。
  - **Maximum timeout for ping** - 从 1 到 10 秒的 ping 超时时间。
  - **启用代理 IP 地址刷新 (Enable agent IP refresh)** - 选中可启用 VLAN 更改检测。
  - **DHCP renew delay** - 代理在 IP 刷新之后等待的秒数。如果启用了 Enable Agent IP Refresh，请配置此值。如果该值不是 0，则代理将在此预期的过渡期间进行一次 IP 刷新。如果在刷新时检测到 VPN，则刷新将被禁用。有效值为 0 到 60 秒，推荐值为 5 秒。
  - **DHCP release delay** - 代理延迟进行 IP 刷新的秒数。如果启用了 Enable Agent IP Refresh，请配置此值。如果该值不是 0，则代理将在此预期的过渡期间进行一次 IP 刷新。如果在刷新时检测到 VPN，则刷新将被禁用。有效值为 0 到 60 秒，推荐值为 5 秒。
  - **Network transition delay** - 代理暂停网络监控以便等待计划好的 IP 更改的时间范围（以秒为单位）。推荐值为 5 秒。

- **终端安全评估协议**
  - **Discovery host** - 代理可以连接的服务器。对于独立配置文件编辑器，仅输入单个主机。
  - **Server name rules** - 由通配符、逗号分隔名称组成的列表，用于定义代理可以连接到的服务器（如 .cisco.com）。
  - **Call Home List** - 输入您想用于负载均衡、监控和故障排除查找的 FQDN，或者您想用于映射到该节点中默认策略服务节点 (PSN) 的 DNS 的 FQDN（如果处于多重情形下）。在配置此选项后，将发送用于监控和故障排除查找的第一次探测，以拨打住宅电话。在从重定向网络迁移到非重定向网络时，必须配置此选项。

- **PRA retransmission time** - 当发生被动重新评估通信失败时，就会指定此代理重试时间范围。有效范围为 60 到 3600 秒。
- **重新传输延迟** — 指定重试之前的等待时间（以秒为单位）。有效范围是从 5 到 300 秒。
- **重新传输限制** — 指定允许对邮件执行的重试次数。有效范围为 0 到 10。

高级面板

AnyConnect 安全移动客户端 UI 的高级面板是每个组件显示统计信息、用户首选项和特定于组件的任何其他信息的区域。如果单击 AnyConnect 系统托盘上的**所有组件的高级窗口 (Advanced Window for all components)** 图标，则新的“系统扫描”(System Scan) 部分将包含以下选项卡：

注释 这些统计信息、用户首选项、消息历史记录等等均显示在 macOS 的“统计信息”(Statistics) 窗口下面。首选项在“首选项”(Preferences) 窗口中，而不像在 Windows 中那样在选项卡中。

- **首选项 (Preferences)** — 允许您阻止与不受信任的服务器的连接，以便在下载程序过程中，对于任何具有不受信任的认证且未经验证的 ISE 服务器，您都会收到“已阻止不受信任的服务器”(Untrusted Server Blocked) 消息。如果禁用阻止，AnyConnect 不会阻止与潜在恶意网络设备的连接。
- **Statistics**（**统计**）— 提供当前 ISE 终端安全评估状态（合规或不合规）、OPSWAT 版本信息、可接受使用策略的状态、终端安全评估的最新运行时间戳、所有缺少的要求以及对故障排除来说足够重要而要显示的任何其他统计信息。
- **Security Products**（**安全产品**）— 访问系统中安装的防恶意软件产品的列表。
- **Scan Summary**（**扫描摘要**）— 允许用户查看管理员为其配置以供查看的任何终端安全评估项。例如，配置时，他们可以查看查看显示终端安全评估的所有项或者只查看终端安全评估检查和要求的补救失败的项。
- **Message History**（**消息历史**）— 为组件提供向系统托盘发送的每条状态消息的历史记录。该历史记录对于故障排除非常有用。

VPN 终端安全评估 (HostScan) 模块提供的功能

HostScan

HostScan 是在用户连接到 ASA 后但在登录前安装到远程设备上的软件包。HostScan 由基本模块、终端评估模块和高级终端评估模块任意组合而成。HostScan 不支持移动设备（Android、iOS、Chrome 或 UWP）。

注释 在 AnyConnect 版本 3.x 中，此软件包捆绑在 hostscan_version.pkg 文件中，必须在 ASA 中的 HostScan 映像下更新并启用该文件才能获得 HostScan 功能。此软件包当前单独安装。

基本功能

HostScan 在建立思科无客户端 SSL VPN 或 AnyConnect 客户端会话的任何远程设备上自动识别操作系统和服务包。

您还可以配置 HostScan 以检查终端的特定流程、文件和数字密钥。它在全隧道建立之前执行上述所有检查项，然后向 ASA 发送此信息以区分公司拥有的计算机、个人计算机和公共计算机。该信息也可用于评估。

注释 登录前评估信息和返回的证书信息不可用。HostScan 不是身份验证方法。它只是检验尝试连接的设备上存在什么。

HostScan 也会自动返回以下其他值，用于根据已配置的 DAP 终端条件进行评估：

- Microsoft Windows、macOS 和 Linux 操作系统
- Microsoft 知识库编号 (KB)
- 设备终端属性类型（如：主机名、MAC 地址、BIOS 序列号、端口号（传统属性）、TCP/UDP 端口号、隐私保护和终端评估（OPSWAT）的版本

注释 HostScan 会收集有关 Windows 客户端系统上 Microsoft 软件更新的服务版本 (GDR) 信息。服务版本包含多个修补程序。服务版本终端属性用在 DAP 规则（而非修补程序）中。

终端评估

终端评估是一项 HostScan 扩展功能，用于检查远程计算机上是否存在大量防病毒和反间谍软件应用、相关定义更新以及防火墙。在 ASA 向会话分配特定动态访问策略 (DAP) 之前，可以使用此功能组合终端条件来满足您的要求。

有关详细信息，请参阅相应版本的思科 ASA 系列 VPN 配置指南中的动态访问策略部分。

高级终端评估：防恶意软件和防火墙补救

在 Windows、macOS 和 Linux 桌面中，如果软件允许单独的应用启动补救，高级终端评估可以尝试发起防恶意软件和个人防火墙保护等各方面的补救。

防恶意软件 - 高级终端评估可以尝试补救防恶意软件的以下组件：

- 强制文件系统保护 - 如果防恶意软件已被禁用，则高级终端评估将启用它。

- 强制病毒定义更新 - 如果在高级终端评估配置定义的天数内未更新防恶意软件定义，则高级终端评估将尝试发起病毒定义更新。

个人防火墙 - 高级终端评估模块可以启用或禁用防火墙。

HostScan 版本 4.4 不支持阻止或允许使用个人防火墙的应用和端口。

注释 并非所有个人防火墙都支持此 Force Enable/Force Disable 功能。

为 HostScan 配置防恶意软件应用

在安装 VPN 终端安全评估 (HostScan) 模块之前，请配置您的防恶意软件，将以下这些应用归为安全例外。防恶意软件应用可能会将这些应用的行为误判为恶意行为：

- cscan.exe
- ciscod.exe
- cstub.exe

与动态访问策略集成

ASA 将 HostScan 功能集成到动态访问策略 (DAP) 中。根据配置，ASA 将一个或多个终端属性值与可选 AAA 属性值组合作为分配 DAP 的条件。DAP 的终端属性支持的 HostScan 功能包括操作系统检测、策略、基本结果和终端评估。

可以指定单个属性或组合多个属性来构成将 DAP 分配到会话所需的条件。DAP 提供适用于终端 AAA 属性值级别的网络访问。当满足所有已配置的终端条件后，ASA 应用 DAP。

请参阅思科 ASA 系列 VPN 配置指南中的配置动态访问策略部分。

DAP 中的 BIOS 序列号

VPN 终端安全评估 (HostScan) 可以检索主机的 BIOS 序列号。您可以使用动态访问策略 (DAP) 允许或阻止基于该 BIOS 序列号建立到 ASA 的 VPN 连接。

将 BIOS 指定为 DAP 终端属性

步骤 1 登录到 ASDM。

步骤 2 选择**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** 或**无客户端 SSL VPN 访问 (Clientless SSL VPN Access)** > **动态接入策略 (Dynamic Access Policies)**。

步骤 3 在“配置动态访问策略”(Configure Dynamic Access Policies) 面板中，单击**添加 (Add)** 或**编辑 (Edit)** 将 BIOS 配置为 DAP 终端属性。

步骤 4 在“终端 ID”(Endpoint ID) 表的右侧，单击**添加 (Add)**。

步骤 5 在“终端属性类型”(Endpoint Attribute Type) 字段中，选择**设备 (Device)**。

步骤 6 选中 **BIOS 序列号 (BIOS Serial Number)** 复选框，选择 **=**（等于）或 **!=**（不等于），然后在“BIOS 序列号”(BIOS Serial Number) 字段中输入 BIOS 编号。单击**确定 (OK)** 保存在“终端属性”(Endpoint Attribute) 对话框中的更改。

步骤 7 单击**确定 (OK)** 保存对“编辑动态访问策略”(Edit Dynamic Access Policy) 的更改。

步骤 8 单击**应用 (Apply)** 保存对动态访问策略的更改。

步骤 9 单击**保存 (Save)**。

如何获取 BIOS 序列号

- Windows - http://support.microsoft.com/kb/558124
- macOS—http://support.apple.com/kb/ht1529
- Linux - 使用此命令：

```
/usr/bin/hal-get-property --udi /org/freedesktop/Hal/devices/computer --key
system.hardware.serial
```

确定在 ASA 上启用的 HostScan 映像

打开 ASDM 并选择 **配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > HostScan 映像 (HostScan Image)**。

升级 HostScan

如果您要手动升级 AnyConnect 和 HostScans（使用 msiexec），请确保先升级 AnyConnect，然后再升级 HostScan。

OPSWAT 支持

AnyConnect 的 VPN (Hostscan) 终端安全评估和 ISE 终端安全评估模块均使用 OPSWAT 框架来保护终端。

此框架涉及客户端和头端，可协助评估终端上的第三方应用。在客户端和头端中使用的 OPSWAT 版本必须匹配。每种终端安全评估方法都提供了支持图表，其中包含了与所用 OPSWAT 版本识别的应用列表对应的产品和版本信息。

当头端（ASA 或 ISE）和终端（VPN 终端安全评估或 ISE 终端安全评估）之间存在版本号不匹配的情况时，OPSWAT 合规性模块将会进行升级或降级，以便与头端上的版本匹配。这些升级/降级是强制性的，并会自动进行，无需最终用户干预，只要建立了到头端的连接即可。

VPN Hostscan 终端安全评估 OPSWAT 支持

HostScan 支持图表 与 HostScan 软件包版本相对应，该版本在与 ASA 头端配合使用的 AnyConnect 中提供 HostScan 终端安全评估。

HostScan 的版本将与 AnyConnect 的主版本和维护版本保持协调。在 ASDM 的**配置 > 远程接入 VPN > 安全桌面管理器 > 主机扫描映像**中配置 HostScan 软件包时，指定 HostScan 版本。

VPN HostScan 终端安全评估准则：

- 所有 4.3.x 以下（包括 4.3.x）版本的 HostScan 都使用 OPSWAT v2。HostScan 4.6 x 和更高版本使用 OPSWAT v4。所有版本的 HostScan 都不支持 OPSWAT v3。
- AnyConnect 4.4.x 和 4.5.x 支持 HostScan 版本 4.3.05017 和更高版本。HostScan 没有 4.4.x 或 4.5.x 版本。
- AnyConnect 4.6.x 支持 HostScan 4.3.05050 （及更高的 4.3.x 版本）以及 4.6.x 版本。
- AnyConnect 4.7.x 支持 HostScan 4.3.05050 （及更高的 4.3.x 版本）以及 4.7.x 版本。
- AnyConnect 4.8.x 支持 HostScan 4.3.05050 （及更高的 4.3.x 版本）以及 4.8.x 版本。
- 由于底层 OPSWAT 版本变更，必须执行迁移过程，将 HostScan 从 4.3.x 版升级至 4.6.x 及更高版本。在加载 4.6.x 及更高版本的 HostScan 映像以启动迁移时，必须在前端上安装 ASDM 7.9.2 或更高版本以及 HostScan 版本 4.3.05050（或更高的 4.3.x 版） 。

下表详细说明了 HostScan 4.3.05017 和更高版本所用的 OPSWAT 版本。此外还提供了兼容的 AnyConnect 版本、ASA/ASDM 头端要求和可能的降级/升级操作，用于显示共同执行 VPN/HostScan 终端安全评估的产品之间的关系。

OPSWAT 版本	支持的 HostScan 版本	兼容的 AnyConnect 版本	所需的 ASA/ASDM 头端版本	降级/升级操作
v2	4.3.05017 至 4.3.05050 版（包括 4.3.05050 版）	AnyConnect 4.4.x 和 4.5x	支持 AnyConnect 的所有版本。	降级到任何更低的 4.3.x 版 HostScan。 升级到任何更高的 4.3.x 版 HostScan。
	4.3.05050 版，以及所有更高的 4.3.x 版本。	AnyConnect 4.4.x、4.5.x 和 4.6.x	支持 AnyConnect 的所有版本。	降级到任何更低的 4.3.x 版 HostScan。 升级到任何更高的 4.3.x 版 HostScan。 注释 升级到任何 4.6.x 版 HostScan 都要求执行迁移过程。 迁移过程要求在头端上安装 HostScan 4.3.05050（或更高的 4.3.x 版本）。

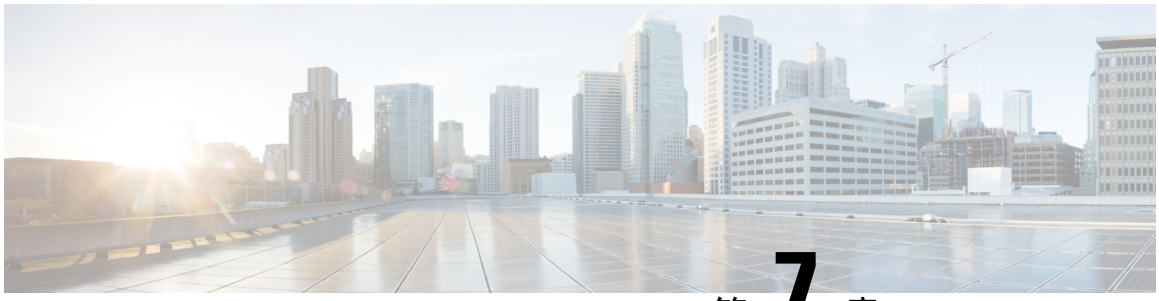
OPSWAT 版本	支持的 HostScan 版本	兼容的 AnyConnect 版本	所需的 ASA/ASDM 头端版本	降级/升级操作
V4	4.6.x	AnyConnect 4.4.x、4.5.x 和 4.6.x	所有支持 AnyConnect 以及 ASDM 7.9.2 或更高版本的 ASA 版本。	降级到任何更低的 4.6.x 版本。 降级到迁移起始版本 4.3.x HS 需要执行回退过程。 升级到任何更高版本。
	4.7.x	AnyConnect 4.4.x、4.5.x、4.6.x 和 4.7.x	所有支持 AnyConnect 以及 ASDM 7.9.2 或更高版本的 ASA 版本。	降级到任何早期 4.7.x 版本。 降级到迁移起始版本 4.3.x HS 需要执行回退过程。 升级到任何更高版本。

ISE 终端安全评估 OPSWAT 支持

思科 AnyConnect 代理合规性模块适用于 ISE 终端安全评估模块。

ISE 代理合规性模块版本反映了基础 OPSWAT 版本。在 ISE 终端安全评估中，OPSWAT 二进制文件封装在一个单独的安装程序中。您可以手动将 OPSWAT 库从本地文件系统载入 ISE 头端，或配置 ISE 使用 ISE 更新源 URL 直接获取该库。

将 AnyConnect 版本 4.3（或更高版本）与 ISE 2.1（或更高版本）配合使用时，可以选择将 OPSWAT v3 或 v4 用于 ISE 合规性模块。防恶意软件的配置位于 ISE UI 的 **Work Centers > Posture > Posture Elements > Conditions > Antimalware**。



第 7 章

配置 AMP Enabler

关于 AMP 启用程序

AnyConnect AMP 启用程序用作为终端部署高级恶意软件防护 (AMP) 的介质。它将面向终端的 AMP 软件从企业中本地托管的服务器推送到一个终端设备子集，并将 AMP 服务安装到现有用户群中。此方法为 AnyConnect 用户群管理员提供了额外的安全代理，可以检测网络中可能发生的潜在恶意软件威胁、删除这些威胁并保护企业免受危害。它能节省带宽和下载时间，不需要在门户端进行任何更改，而且无需向终端发送身份验证凭证即可完成操作。

AMP 启用程序部署

您可以在不需要系统管理员权限的情况下安装 AMP 代理。为了恰当地分发面向终端的 AMP 软件，必须完成以下工作流程。

1. 登录面向终端的 AMP 门户。
2. 在面向终端的 AMP 门户上配置适当的策略。根据您设置的策略，将创建相应的面向终端的 AMP 软件包。该软件包是适用于 Windows 的 .exe 文件或适用于 macOS 的 .pkg 文件。对于 Windows，您可以选择可再分发的 .exe 文件。

   注释 仅支持从端口 443 下载 AMP 连接器。

3. 将生成的套件（Windows 或 macOS）下载到本地服务器中。
4. 登录 ASA 或 ESS 前端创建并保存 AMP 启用程序配置文件。

注释 我们建议您仅为一个头端（ASA 或 ISE）配置该配置文件，尤其是在使用 ISE 终端安全评估时。

5. 在 ASA 或 ESS 前端上，从可选模块列表中选择 AMP 启用程序模块并指定 AMP 启用程序配置文件。

   您创建的配置文件将用于 AnyConnect AMP 启用程序。AMP 启用程序连同此配置文件一起从 ASA 或 ESS 前端被推送到终端。

AMP 启用程序配置文件编辑器

管理员可以选择使用独立编辑器创建 AMP 启用程序配置文件，然后将此配置文件上传到 ASA。否则，会在 Policy Elements 下的 ISE UI 中或在 ASDM 中配置嵌入式 AMP 启用程序配置文件编辑器。为使本地 Web 服务器与 AMP 配置文件编辑器结合使用，必须使用 keytool 命令将根 CA 证书导入到 Java 证书库中：

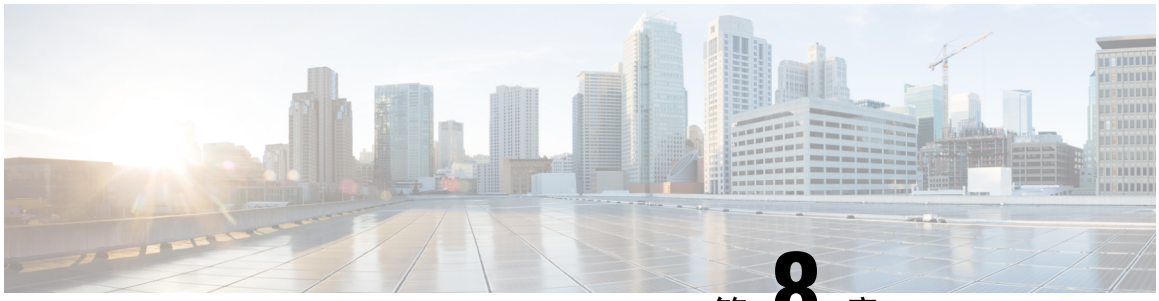
对于 Windows - keytool -import -keystore [JAVA-HOME]/lib/security/cacerts -storepass changeit -trustcacerts -alias root -file [PATH_TO_THE_CERTIFICATE]/certnew.cer

对于 macOS—sudo keytool-import-keystore [JAVA-HOME]/lib/security/cacerts -storepass changeit -trustcacerts -alias root -file [PATH_TO_THE_CERTIFICATE]/certnew.cer

- 名称
- 说明
- “为终端安装 AMP”(Install AMP for Endpoints) - 选择是否要将此配置文件配置为安装适用于终端的 AMP。
- “为终端卸载 AMP”(Uninstall AMP for Endpoints) - 选择是否要将此配置文件配置为卸载适用于终端的 AMP。如果选择卸载，则在其他字段中不应有任何输入。
- Windows Installer - 输入 .exe 文件所在的本地托管服务器地址或 URL。
- “Mac 安装程序”(Mac Installer) - 输入 .pkg 文件所在的本地托管服务器地址或 URL。
- “检查”(Check) - 单击运行对 URL 的检查以确保其有效。有效 URL 是可访问并包含受信任证书的 URL。如果服务器可访问，并且在此 URL 建立了连接，则可以保存配置文件。
- “添加到启动菜单”(Add to Start Menu) - 创建“开始”(Start) 菜单快捷方式。
- “添加到桌面”(Add to Desktop) - 创建桌面图标。
- “添加到情景菜单”(Add to Context Menu) - 如果选择此选项，则可以从任何文件或文件夹右键单击，然后选择 “开始扫描”(Scan Now) 激活扫描。

AMP 启用程序的状态

任何与实际下载和安装 AMP 相关的消息都显示为 AnyConnect 用户界面的 AMP Enabler 磁贴中的部分磁贴。安装后，所有与 AMP 相关的消息都位于 AMP 中，可在终端用户界面中显示。例如，当防恶意软件保护安装或卸载时，如果收到任何出现故障或需要重新启动的指示，用户就会看到消息。



第 8 章

网络可视性模块

关于网络可视性模块

由于用户越来越多地在非托管设备上操作，因此企业管理员对网络内部和外部的可视性下降。网络可视性模块 (NVM) 可以从本地或外部终端收集丰富的流上下文信息；当与 Stealthwatch 等思科解决方案或 Splunk 等第三方解决方案配合使用时，它能够提供对网络连接设备和用户行为的可视性。然后，企业管理员可以执行容量和服务规划、审计、合规性检查和安全性分析。NVM 提供以下服务：

- 通过监控应用的使用情况，更好地依据事实改进网络设计（对 nvzFlow 协议规范中的 IPFIX 收集器元素加以扩展：https://developer.cisco.com/site/network-visibility-module/）。
- 对应用、用户或终端进行逻辑分组。
- 通过查找潜在异常，帮助跟踪企业资产并规划迁移活动。

利用此功能，您可以选择是否不将整个基础设施部署作为遥测对象。NVM 可收集终端遥测信息，提高以下内容的可视性：

- 设备 - 终端，不考虑其位置
- 用户 - 登录到终端的用户
- 应用 - 生成流量的应用
- 位置 - 生成流量的网络位置
- 目的地 - 流量发往地的实际域名 (FQDN)

在一个受信任的网络中，AnyConnect NVM 将流记录导出到收集器（例如思科 Stealthwatch）或第三方供应商（例如 Splunk），由其进行文件分析并提供 UI 接口和报告。流记录提供关于用户功能的信息，相关值按 ID 导出（例如 LoggedInUserAccountType 导出为 12361，ProcessUserAccountType 导出为 12362，ParentProcessUserAccountType 导出为 12363）。有关在 Splunk 上构建的思科终端安全分析 (CESA) 的详细信息， 请参阅 http://www.cisco.com/go/cesa。由于大多数企业 IT 管理员可能需要利用该数据构建各自的可视化模板，因此我们通过 Splunk 应用插件提供了一些示例基础模板。

桌面 AnyConnect 上的 NVM

过去，流量收集器提供相应功能来收集出入交换机或路由器的一个接口的 IP 网络流量。它可以确定网络中的拥塞来源、流量路径，但没有多少其他信息。在终端上使用 NVM 时，会通过丰富的终端上下文（如设备类型、用户、应用等）来增强流。这将使流记录更具可操作性，具体取决于收集平台的功能。通过 IPFIX 发送的 NVM 所提供的导出数据与思科 NetFlow 收集器以及其他第三方流收集平台（如 Splunk、IBM Qradar、LiveAction）兼容。有关其他信息，请参阅特定于平台的集成文档，例如，可访问以下网址了解 Splunk 集成的信息：
https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200600-Install-and-Configure-Cisco-Network-Visi.html。

在版本 4.9 或更高版本中使用 NVM 收集器时，您必须使用 Splunk 应用 3.x 查看其他参数。

如果此功能为启用状态，NVM 的 AnyConnect 配置文件将从 ISE 或 ASA 头端推送。与您在网络访问管理器上的操作一样，在 ISE 头端，您可以使用独立配置文件编辑器，生成 NVM 服务配置文件 XML，上传至 ISE 并对照新的 NVM 模块进行映射。在 ASA 头端，您可以使用独立配置文件编辑器或 ASDM 配置文件编辑器。

当 VPN 状态更改为已连接，或者当终端处于受信任的网络中时，NVM 会收到提示。

注释 如果您将 NVM 与 Linux 一起使用，请确保已完成在 Linux 上使用 NVM，第 7 页中的预备步骤。

独立 NVM

对于没有 AnyConnect 部署或正在使用其他 VPN 解决方案的用户，您可以安装 NVM 独立软件包以满足您的 NVM 需求。此软件包独立运行，但它提供与现有 AnyConnect NVM 解决方案相同的流收集级别。如果安装独立 NVM，活动进程（例如 MacOS 上的活动监视器）指出其使用情况。

独立 NVM 使用NVM 配置文件编辑器，第 94 页进行配置，且值得信赖的网络检测 (TND) 配置为必填项。使用 TND 配置，NVM 确定终端是否在企业网络上，然后应用适当的策略。

故障排除和日志记录仍通过 AnyConnect DART （可从 AnyConnect 软件包进行安装）完成。

部署模式

您可以通过以下两种方式之一部署 NVM：1) 使用 AnyConnect 软件包，或 2) 使用独立的 NVM 软件包（仅限 AnyConnect 桌面）。有关将部署为 AnyConnect 软件包的一部分的步骤，请参阅 "部署 *AnyConnect* " 一章。否则，您最初可以通过下载以下软件包来安装独立 NVM，而无需完整的 AnyConnect 软件包：

- anyconnect-win-[version]-nvm-standalone-k9 （适用于 Windows）
- anyconnect-macos-[version]-nvm-standalone. dmg （适用于 macOS）
- anyconnect-linux64-[version]-nvm-standalone. tar gz （适用于 Linux）

独立 NVM 的正常运行不依赖于 VPN；因此，您可以将其部署在终端上，而无需安装 VPN。

如果已安装独立 NVM，则可以无缝地迁移到相同或更高版本的完整 AnyConnect 安装，并且所有 NVM 数据文件和配置文件都将保留。

要升级到 NVM 独立配置，必须将带外方法（例如 SMS）用于 NVM 配置文件。如果在终端上同时需要 VPN 和 NVM 功能，我们建议您部署 AnyConnect 软件包以安装 VPN 和 NVM，因为不建议进行单独安装。在以下情况下，安装将失败：

- 降级独立 NVM
- 使用 NVM 安装较旧版本的 AnyConnect VPN，其中已存在较新版本的独立 NVM。这种情况会导致卸载独立 NVM。
- 安装任何版本的独立 NVM，其中 AnyConnect VPN 和 NVM 已存在

移动 AnyConnect 上的 NVM

Android 版 Cisco AnyConnect Secure Mobility Client 版本 4.0.09xxx（可通过 Google playstore 获取）中包括网络可见性模块 (NVM)。运行 Samsung Knox 版本 2.8 或更高版本的 Samsung 设备上支持 NVM。目前不支持任何其他移动设备。

Android 上的网络可见性是服务配置文件配置的一部分。要在 Android 上配置 NVM，需使用 AnyConnect NVM 配置文件编辑器生成 AnyConnect NVM 配置文件，然后再使用移动设备管理 (MDM) 将该配置文件推送到 Samsung 移动设备。需要有 AnyConnect 版本 4.4.3 或更高版本中的 AnyConnect NVM 配置文件编辑器，才能为移动设备配置 NVM。

指南

- 运行 Samsung Knox 版本 3.0 或更高版本的 Samsung 设备上支持 NVM。目前不支持任何其他移动设备。
- 在移动设备上，支持通过 IPv4 或 IPv6 连接到收集器。
- 不支持在基于 Java 的应用上收集数据流量。

如何使用 NVM

您可以将 NVM 用于以下场景：

- 在发生安全事件后，审核用户网络历史记录的潜在泄露。
- 查看系统或管理权限如何影响在用户的设备上正在运行且连接网络的进程。

- 获取运行旧版操作系统的所有设备的列表。
- 确定您的网络中的哪些应用正在占用最高的网络带宽。
- 确定您的网络中正在使用多少个 Firefox 版本。
- 确定您的网络中 IPv6 占 Chrome.exe 连接的百分比。

NVM 的收集参数

在三个系统日志数据源：每一数据流、终端身份和接口信息中，唯一标识符 (UDID) 字段可用作关联这些源之间记录的方式。您可以使用 InterfaceInfoUDID 字段将每一数据流记录与接口信息记录相关联，以便收集有关该特定接口的详细信息。以下参数在终端收集并导出到收集器：

表 *7:* 终端身份

参数	说明/注释
虚拟站名称	在终端上配置的设备名称（例如，Boris-Macbook） 加入域的计算机将采用以下格式：<machinename>.<domainname>.<com>（例如，CESA-WIN10-1.mydomain.com） 对 Android 为空；Samsung 未提供。
UDID	通用唯一标识符。唯一标识与每个流量对应的终端。此 UDID 值还通过桌面中的 HostScan 和移动设备中的 ACIDex 报告。
操作系统名称	终端操作系统的名称（例如，WinNT）
OS 版本	终端操作系统的版本（例如，6.1.7601）
操作系统版本	操作系统版本，例如 Windows 8.1 Enterprise Edition
系统制造商	终端制造商（例如，联想、苹果等）
系统类型	针对 Android 设置为 `arm`。 针对其他平台，设置为 `x86` 或 `x64`。
代理版本	终端上运行的 NVM 客户端软件的版本。格式通常为 major_v.minor_v.build_no

表 *8:* 接口信息

参数	说明/注释
终端 UDID	与 UDID 相同。

参数	说明/注释
InterfaceInfoUID	接口元数据的唯一 ID。用于从 InterfaceInfo 记录查找接口元数据。
接口索引	操作系统报告的网络接口索引。
接口类型	接口类型，例如有线、无线、蜂窝、VPN 等。
接口名称	操作系统报告的网络接口/适配器名称。
接口详细信息列表	状态和 SSID，InterfaceDetailsList 的属性。表示接口的网络状态（受信任或不受信任），以及连接的 SSID。
接口 MAC 地址	接口的 MAC 地址。 仅限桌面。对 Android 为空（不受支持）。

表 *9:* 流信息

参数	说明/注释
源 IPv4 地址	终端上生成流的源接口的 IPv4 地址。
目的 IPv4 地址	终端上生成流的目标接口的 IPv4 地址。
源传输端口	终端上生成流的源端口号。
目标传输端口	终端上生成流的目标端口号。
源 IPv6 地址 (Source IPv6 Address)	终端上生成流的源接口的 IPv6 地址。 对 Android 为空（不受支持）。
目的 IPv6 地址 (Destination IPv6 Address)	终端上生成流的目标接口的 IPv6 地址。 对 Android 为空（不受支持）。
开始秒 结束秒	流量开始或结束的绝对时间戳（以秒为单位）。
开始（毫秒） 结束（毫秒）	流量开始或结束的绝对时间戳（以毫秒为单位）。
流量 UDID	与 UDID 相同。
当前登录用户	物理设备上登录的用户名，格式为“机构\主体” 对 Android 为空（不受支持）。

参数	说明/注释
已登录用户帐户类型	已登录用户的帐户类型。 对 Android 为空（不受支持）。
进程 ID	发起网络流的进程的进程 ID。
进程名称	在终端上生成网络流的可执行文件名称。
进程散列	在终端上生成网络流的可执行文件的唯一 SHA256 哈希值。
进程帐户	在终端上生成网络流的应用执行情景所属的完全限定帐户，格式为“机构\主体”。 对 Android 为空（不受支持）。
进程帐户类型	进程帐户的帐户类型。 对 Android 为空（不受支持）。
进程路径	发起网络流的进程的文件系统路径 对 Android 为空（不受支持）。
进程参数	发起网络流的进程的命令行参数，不包括进程路径。 对 Android 为空（不受支持）。
父进程 ID	发起网络流的进程的父进程 ID。
父进程名称	在终端上生成网络流的应用的父进程名称。
父进程哈希值	在终端上生成网络流的应用的父进程可执行文件的唯一 SHA256 哈希值。针对 Android 设置为 0。
父进程帐户	在终端上生成网络流的应用父进程执行情景所属的完全限定帐户，格式为“机构\主体”。 对 Android 为空（不受支持）。
父进程帐户类型	父进程帐户的帐户类型。 对 Android 为空（不受支持）。
父进程路径	发起网络流的进程父级的文件系统路径。 对 Android 为空（不受支持）。
父进程参数	发起网络流的进程父级的命令行参数，不包括父进程路径。 对 Android 为空（不受支持）。
DNS 后缀	在终端上与流量关联的接口上配置。

参数	说明/注释
L4ByteCountIn	在第 4 层终端（不包括 L4 信头）上的给定流中下载的总字节数。
L4ByteCountOut	在第 4 层终端（不包括 L4 信头）上的给定流中上传的总字节数。
目标主机名	在终端上解析为目标 IP 的实际 FQDN
接口 UID	与接口信息表中的接口 UID 相同。用于从连同 UDID 一起发送的接口记录中识别此流的接口信息。
模块名称列表	生成流的进程托管的模块的名称（0 个或更多）列表。其中可包括公共容器中的主要 DLL，例如 dllhost、svchost、rundll32 等。它还可以包含其他托管组件，例如 JVM 中 jar 文件的名称。 对 Android 为空（不受支持）。
模块哈希值列表	与模块名称列表关联的模块的 SHA256 哈希值（0 个或更多）列表。 对 Android 为空（不受支持）。

NVM 配置文件编辑器

在配置文件编辑器中，配置收集服务器的 IP 地址或 FQDN。您还可以自定义数据收集策略，用于选择要发送哪些类型数据，以及确定数据是否匿名。

网络可视性模块可以使用包含 IPv4 地址的单个堆栈 IPv4、包含 IPv6 地址的单个堆栈 IPv6 或双堆栈 IPv4/IPv6，建立与操作系统首选的 IP地址的连接。

移动网络可视性模块仅可以使用 IPv4 建立连接。不支持 IPv6 连接。

注释 当网络可视性模块在受信任网络中时，该模块发送流量信息。默认情况下，不收集任何数据。仅在配置文件中进行了相应配置时才会收集数据，且连接终端后，会继续收集数据。如果在一个不可信网络上进行收集，则会缓存数据，并在终端处于受信任的网络中时发送数据。如果您将收集数据发送到 Stealthwatch 7.3.1 及更低版本（或 Splunk 及类似 SIEM 工具之外的工具），则缓存数据会在受信任网络上发送一次，但不会进行处理。对于 Stealthwatch 应用程序，请参阅 Stealthwatch 企业终端许可证和 NVM 配置指南。

如果已在 NVM 配置文件中配置了 TND，则受信任的网络检测由 NVM 完成，并且不依赖于 VPN 来确定终端是否位于受信任的网络中。此外，如果 VPN 为已连接状态，则会将终端视作处于受信任网络中，并会发送流信息。NVM 特定的系统日志会显示 TND 使用情况。

直接在 NVM 配置文件中配置 TND 时，管理员定义的受信任服务器和证书散列将确定用户位于受信任还是不受信任的网络上。管理员为核心 VPN 配置文件配置 TND 会在核心 VPN 配置文件中另外配置受信任 DNS 域和受信任 DNS 服务器：AnyConnect 配置文件编辑器，首选项（第 2 部分），第 79 页。

- **桌面 (Desktop) 或移动 (Mobile)** - 确定是在桌面还是移动设备上设置 NVM。**桌面 (Desktop)** 是默认值。 未来将支持移动设备。
- **收集器配置**
  - **IP 地址/FQDN (IP Address/FQDN)** - 指定收集器的 IPv4 或 IPv6 IP 地址/FQDN。
  - **端口 (Port)** - 指定收集器正在侦听哪个端口号。
  - **安全 (Secure)** - 确定是否希望 NVM 通过 DTLS 安全地将数据发送到收集器。选中此复选框后，NVM 将使用 DTLS 进行传输。DTLS 连接要求终端信任 DTLS 服务器（收集器）证书。系统将以静默方式拒绝任何不受信任的证书。

    DTLS 支持需要收集器作为 CESA Splunk 应用 v3.1.0 的一部分，DTLS 1.2 是支持的最低版本。
- **缓存配置**
  - **最大大小 (Max Size)** - 指定该数据库可以达到的最大大小。以前对缓存大小有预设的限制，但您现在可在配置文件中配置它。缓存中的数据以加密格式存储，因此只有拥有根权限的进程可以解密数据。

    一旦达到大小限制，将从空间中丢弃最旧数据，将空间留给新数据。
  - **最大持续时间 (Max Duration)** - 指定您希望将数据存储多少天。如果您还设置了最大大小，则首先达到的限制优先。

    一旦达到天数限制，将从空间中丢弃日期最早的数据，将空间留给日期最近的数据。如果仅配置了“最大持续时间 (Max Duration)”，则没有大小上限；如果二者都被禁用，则大小上限为 50 MB。
- **定期模板** - 指定从终端发出模板的时间间隔。默认值为 1440 分钟

- **定期流量报告**（可选，仅应用于桌面）- 单击以启用定期流量报告。默认情况下，NVM 发送连接结束时的流量相关信息 （当禁用此选项时）。如果需要定期的流量相关信息（甚至在这些流量被关闭之前），请在此处设置间隔（以秒为单位）。值为 0 表示在每个流量开始和结束时发送流量信息。如果值为 *n*，则将在每个流量开始时、每隔 *n* 秒时和结束时发送流量信息。使用此设置跟踪长期运行的连接（甚至在这些连接被关闭之前）。
- **聚合时间间隔** - 指定从端点导出数据流的时间间隔。使用 5 秒默认值时，一个数据包中将捕获不止一个数据流。如果时间间隔值为 0 秒，则每个数据包都有一个数据流。有效范围为 0 到 600 秒。
- **限制速率 (Throttle Rate)** - 限制控制以什么速率将数据从缓存发送到收集器，以便尽量减小对最终用户的影响。您可以对实时和缓存数据应用限制（只要存在缓存的数据）。以 Kbps 为单位，输入限制速率。默认值为 500 Kbps。

  在该固定时段后，缓存数据将被导出。输入 0 将禁用该功能。
- **收集模式 (Collection Mode)** - 通过选择收集模式关闭 (collection mode is off)、仅受信任网络 (trusted network only)、仅不受信任网络 (untrusted network only) 或所有网络 (all networks)，指定应从终端收集数据的时间。
- **收集标准 (Collection Criteria)** - 您可以在数据收集时减少不必要的广播，以便仅分析相关数据。通过以下选项控制数据搜集：
  - **广播数据包 (Broadcast packets)** 和**组播数据包 (Multicast packets)**（仅适用于桌面）- 默认情况下，为了提高效率，会关闭广播和组播数据包收集，以便缩短在后端资源上花费的时间。单击该复选框可启用对广播和组播数据包的收集并过滤数据。
  - **仅限 KNOX (KNOX only)**（可选且特定于移动设备）- 选中后，将仅从 KNOX 工作空间收集数据。默认情况下，未选中此字段，将会从工作空间内部和外部收集数据。
- **数据收集策略 (Data Collection Policy)** - 您可以添加数据收集策略，并将它们与网络类型或连接情形相关联。您可以将一种策略应用于 VPN，而将另一种策略应用于非 VPN 流量，因为多个接口可以同时处于活跃状态。

  在单击“添加”(Add) 时，系统显示“数据收集策略”(Data Collection Policy) 窗口。在创建策略时，请记住以下指导原则：
  - 默认情况下，如果未创建策略或未与网络类型相关联，则将报告和收集所有字段。
  - 每种数据收集策略必须与至少一种网络类型相关联，但您不能将两种策略与同一种网络类型相关联。
  - 具有更具体的网络类型的策略优先。例如，因为 VPN 是受信任网络的一部分，所以包含 VPN 网络类型的策略的优先级高于采用受信任网络为指定网络的策略。
  - 您只能基于所选的收集型号，为网络创建适用的数据收集策略。例如，如果**收集模式 (Collection Mode)** 设置为 **仅受信任网络 (Trusted Network Only)**，您无法为**不受信任网络类型 (Untrusted Network Type)** 创建**数据收集策略 (Data Collection Policy)**。

- 如果从较新版本的 AnyConnect 打开来自较早版本 AnyConnect 的配置文件，它会自动将该配置文件转换为较新的版本。转换过程中会为所有网络添加数据收集策略，用于排除先前匿名的字段。

- **名称 (Name)** - 为您要创建的策略指定名称。

- **网络类型 (Network Type)** - 通过选择 VPN、受信任或不受信任，来确定收集模式，或者应用数据收集策略的网络。如果您选择受信任网络，则策略也适用于 VPN 案例。

- **流过滤器规则** - 定义一组条件和一个操作，可以在满足所有条件时收集或忽略流。您最多可以配置 25 条规则，每条规则最多可以定义 25 个条件。使用“流过滤器规则”列表右侧的向上和向下按钮调整规则的优先级，并对后续规则给予更高的考虑。单击**添加 (Add)** 设置流过滤器规则的组成要素。

  - 名称 - 流过滤器规则的唯一名称。

  - 类型 - 每个过滤器规则都有“收集”或“忽略”类型。确定满足过滤器规则时要执行的操作（“收集”或“忽略”）。如果收集，则在满足条件时允许流。如果忽略，则丢弃流。

  - 条件 - 为要匹配的每个字段添加一个条目以及一个运算，以确定字段值对匹配项是否应相等或不相等。每个运算都有一个字段标识符和该字段的对应值。该字段区分大小写，除非您在设置过滤器引擎规则时对规则集应用了不区分大小写操作 (EqualsIgnoreCase)。启用后，规则中设置的 Value 字段中的输入不区分大小写。

- **包括/排除**

  - **类型 (Type)** - 确定要在数据收集策略中**包含 (Include)** 或**排除 (Exclude)** 的字段。默认值为**排除 (Exclude)**。所有未选中的字段都收集起来。未选中任何字段时，将收集所有字段。

  - **字段** - 确定要从终端接收哪些信息以及收集哪些字段的数据以满足策略要求。根据网络类型和包含或排除的字段，NVM 将在终端上收集相应数据。

注释 升级期间，如果存在以下情况之一，默认从流信息的报告中排除 ProcessPath、ParentProcessPath、ProcessArgs 和 ParentProcessArgs：

- 如果较旧版本NVM中的配置文件没有数据收集策略或有包含数据收集策略。
- 如果较旧版本 NVM 中的配置文件有排除数据收集策略，并且该配置文件已使用更新的4.9版本配置文件编辑器打开并保存。如果较旧版本NVM中的配置文件有排除数据收集策略，但该配置文件未使用更新的4.9版本配置文件编辑器打开和保存，则包含这四个字段。

如果 NVM 无法计算父进程 ID，则值默认为 4294967295。

FlowStartMsec 和 FlowStopMsec 确定流的纪元时间戳（以毫秒为单位）。

对于 AnyConnect 版本4.4（和更高版本），您现在可以选择接口状态和 SSID，这将指定接口的网络状态为受信任还是不受信任。

- **可选匿名字段 (Optional Anonymization Fields)** - 如果要关联同一终端上的记录，同时保留隐私，请选择所需的字段进行匿名化，它们将作为值的哈希而不是实际值进行发送。字段的子集可用于匿名化。

  标记为包含或排除的字段不可用于匿名；同样，标记为匿名的字段不可用于包含或排除。

- **用于 Knox 的数据收集策略 (Data Collection Policy for Knox)**（**特定于移动设备**）- 该选项用于在选择移动配置文件时指定数据收集策略。要为 Knox 容器创建数据收集策略，请选择“范围”(Scope) 下的**仅 Knox (Knox-Only)** 复选框。除非指定单独的 Knox 容器数据收集策略，否则应用于 Knox 容器流量的设备范围内的数据收集策略也适用于 Knox 容器流量。要添加或删除数据收集策略，请参阅上面的数据收集策略说明。您可以为移动配置文件设置最多 6 个不同的数据收集策略：3 个用于设备，3 个用于 Knox。

- **可接受的使用策略 (Acceptable Use Policy)**（可选且特定于移动设备）- 单击**编辑 (Edit)**，在对话框中为移动设备定义可接受的使用策略。完成后，单击**确定 (OK)**。最多允许 4000 个字符。

  配置NVM后，此消息会显示给用户。远程用户无法选择拒绝NVM活动。网络管理员使用MDM工具控制 NVM。

- **Export on Mobile Network**（**可选且特定于移动设备**）- 指定在设备使用移动网络时，是否允许导出 NVM 流。如果启用（默认值），当显示或后续通过 AnyConnect Android 应用中的 **设置 (Settings)** > **NVM-设置 (NVM-Settings)** > > **将移动数据用于 NVM (Use mobile data for NVM)** 复选框来显示“可接受的用户策略”(Acceptable User Policy) 窗口时，最终用户可以覆盖管理员 。如果取消选中“在移动网络上导出”(Export on Mobile Network) 复选框，当设备使用移动网络时，不会导出 NVM 流，最终用户无法对其进行更改。

- **受信任的网络检测** — 此功能可检测终端是否实际上位于企业网络中。NVM 使用网络状态来确定何时导出 NVM 数据并应用相应的数据收集策略。单击**配置 (Configure)** 以设置受信任的网络检测的配置。SSL 探测会发送到已配置的受信任前端，如果可访问，则前端会使用证书响应。然后，系统将根据配置文件编辑器中的散列设置提取指纹（SHA-256 散列）并将其与之匹配。成功匹配表明终端位于受信任的网络中；但是，如果前端无法访问，或者如果证书散列不匹配，则系统会将终端视为位于不受信任的网络中。

  注释 从内部网络的外部进行操作时，TND 会执行 DNS 请求并尝试与已配置服务器建立 SSL 连接。思科强烈建议使用别名，以确保在内部网络以外使用的机器不会通过这些请求泄露您组织的名称和内部结构。

  如果 TND 未在 NVM 配置文件中配置或如果已安装了 VPN 模块，NVM 会使用 配置值得信赖的网络检测来确定终端是否位于受信任的网络中。如果已安装 VPN 模块并在 NVM 配置文件中配置了 TND，则 NVM 会执行值得信赖的网络检测，即使在 VPN 网络内部也是如此。在以前的版本中，VPN 网络会被默认视为受信任的网络。NVM 配置文件编辑器中的 TND 配置包括以下内容：

  1. **https://** — 输入每个受信任服务器的 URL （IP 地址、FQDN 或端口地址），然后单击**添加 (Add)**）。

     注释 代理后的受信任服务器不受支持。

  2. **证书散列 (SHA-256)** — 如果与受信任服务器的 SSL 连接成功，则系统会自动填充此字段。否则，您可以通过输入服务器证书的 SHA-256 散列并单击**设置 (Set)** 来手动对其进行设置。
  3. **受信任服务器列表** — 通过此过程可以定义多个受信任服务器。（至多 10 个。）由于服务器会按已配置的顺序尝试受信任的网络检测，因此您可以使用**上移**和**移动 |向下**按钮来调整该顺序。如果终端无法连接到第一台服务器，它会尝试连接第二台服务器，依此类推。在对列表中的所有服务器进行尝试后，终端等待 10 秒后会再进行最后一次尝试。当服务器进行身份验证时，系统会视为终端在受信任的网络中。

将配置文件另存为 `NVM_ServiceProfile.xml`。您必须将配置文件准确保存为此名称，否则 NVM 将无法收集和发送数据。

关于流过滤器

添加流过滤器会将当前数据收集策略扩展为仅以字段为中心，其中为每个流中的给定字段配置操作。通过“流过滤器”，您可以创建和应用规则以收集或忽略整个流（而不只是特定的字段），从而只监控感兴趣的流量，可能降低存储要求。

规则条件

- 只有在与流数据匹配时满足规则中指定的所有条件时，规则才匹配。
- 所满足的第一个规则会应用于流。
- 如果过滤策略允许，还会在流上应用其余的数据收集策略（包括/排除字段、匿名字段）。
- 使用多个规则的实例，
  - 如果没有与流数据匹配的规则，不会对流执行任何操作。此时会遵循默认行为，即收集流。
  - 如果规则与流数据匹配，则应用该流规则中指定的操作。不检查后续规则。“NVM 配置文件编辑器，第 94 页流过滤器规则”参数中指定的规则顺序指示出现多个匹配时的优先级。

使用通配符、CIDR 和转义序列支持

输入规则条件时，对于 IP 地址，可以使用通配符或 CIDR 表示法定义更广泛的字段值。此外，还可以在字段值中使用某些转义序列。对于 IP 字段，CIDR/斜线符号可以指定规则应匹配的 IP 地址。例如，“192.30.250.00/16”将匹配有通过应用子网掩码“255.255.0.0”得到的路由前缀“192.30.0.0”的所有地址。对于文本字段，可以使用通配符（* 和 ?）和转义序列（*、\? 和 \\）捕获更广泛的输入。例如，登录用户“Jane*”将匹配以“Jane”开头的所有用户名。

实现流量过滤方案的示例配置

要丢弃特定端口（例如端口 53）上的所有 UDP 流量，请使用忽略类型和两个条件配置流过滤器规则：

- 条件 1：指定流协议等于 UDP。
- 条件 2：指定端口号等于 53。

要仅收集来自一个特定进程（例如 Tor 浏览器）的流量，请使用忽略类型配置过滤器规则，通过添加一个条件丢弃所有其他流：

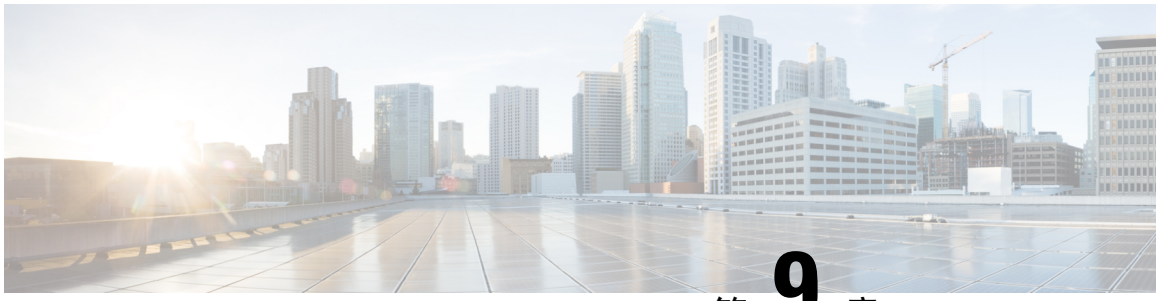
- 条件 1：指定进程名称不等于 Tor 浏览器。

要仅收集源自子网中仅一个特定 IP 的流量，请配置两个规则：

- 规则 1：设置收集类型的规则，条件是 IPv4 源地址等于 192.168.30.14。
- 规则 2：设置忽略类型的第二个规则，条件是 IPv4 源等于 192.168.30.0/24。

客户反馈模块提供 NVM 状态

部分客户反馈模块集合可以提供关于是否已安装 NVM、每日流量和数据库大小等的数据。



第 9 章

Umbrella 漫游安全

Umbrella 漫游安全模块要求订用思科 Umbrella 漫游服务（包含 Professional、Insights、Platform 或 MSP 软件包）。Cisco Umbrella Roaming 在没有 VPN 活动时提供 DNS 层安全保护，而 Cisco Umbrella 订用添加了智能代理。此外，思科 Umbrella 订用还将提供内容过滤、多重策略、稳健性报告、Active Directory 集成等更多功能。无论订用情况如何，都将使用相同的 Umbrella 漫游安全模块。

Umbrella 漫游模块配置文件 (OrgInfo.json) 会将各种部署与相对应的服务关联起来，并将自动启用相对应的保护功能。

可以通过 Umbrella 控制面板实时查看源自漫游安全模块的所有互联网活动。策略和报告中的精细度级别取决于 Umbrella 订用情况。

有关各个服务级别订用中包含哪些功能的详细对比，请参阅 https://umbrella.cisco.com/products/packages。

- 适用于 Android 操作系统的 AnyConnect Umbrella 模块，第 229 页
- 适用于 Windows 或 macOS 的 AnyConnect Umbrella 模块，第 230 页

适用于 Android 操作系统的 AnyConnect Umbrella 模块

适用于 Android 操作系统的 AnyConnect Umbrella 模块是托管的 Android 设备的漫游客户端，它提供 DNS 层保护，这种保护延伸到 Android 工作配置文件所涵盖的应用和浏览。

要将此客户端部署到 Android 设备并将 Umbrella 配置推送到 Android 设备，需要有移动设备管理系统 (MDM)。有关支持的 MDM 和其他前提条件的列表，请参阅在 Android 操作系统上部署 AnyConnect Umbrella 模块的前提条件 。

在 Android 上，某些 AnyConnect 功能在配合 Umbrella 使用时可能功能受限：

- 由于操作系统限制，Per-App VPN 不能与 Umbrella 模块配合使用。如果远程访问 VPN 处于活动状态，Umbrella 只能保护通过 VPN 隧道截获的 DNS 流量。如果为 Per-App VPN 配置了远程访问，则 Umbrella 只能保护隧道应用的 DNS 流量。
- 不应将永远在线 VPN 与锁定 (Fail Close) 选项配合使用。当 VPN 服务器无法接通时，它将停止互联网访问。请参阅您的 MDM 指南，了解如何在永远在线 VPN 设置为“开”时关闭锁定设置。

有关完整的 Umbrella 功能集的说明，请参阅 AnyConnect Umbrella 模块（Android 操作系统）文档。

在 Android 操作系统上部署 AnyConnect Umbrella 模块的前提条件

部署的前提条件：

注释 AnyConnect 监控在 MDM 中创建的工作配置文件内应用和浏览器生成的流量，并相应地阻止或允许浏览。不监控应用和/或浏览器在工作配置文件外生成的任何流量。

- 用于部署软件并将 Umbrella 配置推送到移动设备的移动设备管理系统 (MDM)。当前测试的版本有 Mobile Iron、Meraki、VMWare workspace 1 (Airwatch) 或 Microsoft Intune。
- 安装有 Android OS 6.0.1 及更高版本的 Android (Samsung/Google Pixel) 移动设备。
- 用于配置 DNS 策略、管理注册的 Android 设备以及报告用途的 Umbrella 许可证。
- 用于启用该功能的 Umbrella 组织 ID。
- 对于可信网络检测 (TND)：
  - 如果 Umbrella 模块检测到启用了 HTTPS 的虚拟设备 (VA)，它将自行停用；但是，如果 VA 不支持 HTTPS，则 Umbrella 模块将继续。
  - 必须启用 umbrella_va_fqdns 中的所有 VA FQDN。

适用于 Windows 或 macOS 的 AnyConnect Umbrella 模块

Umbrella 漫游客户端与 Umbrella 漫游安全模块不兼容

Umbrella 漫游安全模块与 Umbrella 漫游客户端不兼容。如果您要部署 Umbrella 漫游安全模块，在安装漫游安全模块过程中将检测任何现已安装的 Umbrella 漫游客户端并自动删除，以防止冲突。如果现已安装的 Umbrella 漫游客户端与某项 Umbrella 服务订用相关联，会将该项服务订用自动迁移至 Umbrella 漫游安全模块，除非 OrgInfo.json 文件与配置用于网络部署或预部署的 AnyConnect 安装程序处于 Umbrella 模块目录中的同一位置。您也可能希望在部署 Umbrella 漫游安全模块之前手动卸载 Umbrella 漫游客户端。

获得思科 Umbrella 帐户

Umbrella 控制面板 (http://dashboard.umbrella.com/) 是登录页面，您可在此获得用于要包括在您的部署中的 AnyConnect Umbrella 漫游安全模块的配置文件 (OrgInfo.json)。您还可以在此对漫游客户端活动的策略和报告进行管理。

从控制面板下载 OrgInfo 文件

OrgInfo.json 文件包含关于您的 Umbrella 控制面板实例的具体信息，可让漫游安全模块了解向哪里报告，以及需要实施哪些策略。

要为部署 AnyConnect Umbrella 漫游安全模块做好准备，请从 Umbrella 控制面板获取 OrgInfo.json 文件 (https://dashboard.umbrella.com)。

单击“身份 (Identities)”菜单结构中的**漫游计算机 (Roaming Computers)**，然后单击页面左上角的 + 符号。向下滚动到 AnyConnect Umbrella 漫游安全模块并单击**模块配置文件 (Module Profile)**。有关具体说明/部署步骤以及软件包和文件的具体信息，请参阅 AnyConnect 部署概述，第 2 页。

注释 在首次部署 OrgInfo.json 文件时，会将该文件复制到数据子目录 (/umbrella/data) 中，还会在该子目录中创建几个其他注册文件。因此，如果您需要部署替代 OrgInfo.json 文件，则必须删除该数据子目录。或者，您也可以卸载 Umbrella 漫游安全模块（这将删除该数据子目录），然后使用新 OrgInfo.json 文件重新安装。

安装和运行 Umbrella 漫游安全

在部署 AnyConnect 时，Umbrella 漫游安全模块是您可以引入以启用额外功能的众多可选模块之一。

要解释 Umbrella 安全模块的状态和条件，请参阅 AnyConnect 插件：Umbrella 漫游安全客户端管理员指南。

配置 OrgInfo.json 文件

OrgInfo.json 文件包含关于您的 Umbrella 服务订用的具体信息，可让安全漫游模块了解向哪里报告，以及需要实施哪些策略。可以使用 CLI 或 GUI 从 ASA 或 ISE 来部署 OrgInfo.json 文件并启用 Umbrella 漫游安全模块。下面的步骤首先描述了如何从 ASA 启用，然后描述了如何从 ISE 启用：

ASA CLI

1. 将您从 Umbrella 控制面板 (https://dashboard.umbrella.com) 获得的 OrgInfo.json 上传到 ASA 文件系统。
2. 发布以下命令，针对您的配置根据需要调整组策略名称。

```
webvpn
 anyconnect profiles OrgInfo disk0:/OrgInfo.json

group-policy DfltGrpPolicy attribute
 webvpn
  anyconnect profiles value OrgInfo type umbrella
```

ASDM GUI

1. 导航到**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（客户端）访问 (Network [Client] Access) > AnyConnect 客户端配置文件 (AnyConnect Client Profile)**。

2. 选择**添加 (Add)**。
3. 为简档命名。
4. 从“配置文件用途”(Profile Usage) 下拉菜单中选择 Umbrella 安全漫游客户端类型。OrgInfo.json 文件将填充在 Profile Location 字段中。
5. 单击**上传 (Upload)**，然后浏览到您从控制面板下载的 OrgInfo.json 文件的位置。
6. 将其与 Group Policy 下拉菜单上的 DfltGrpPolicy 关联起来。请参阅启用其他 AnyConnect 模块，第 23 页以在组策略中指定新模块名称。

ISE

按照以下步骤操作，以从 ISE 启用：

1. 上传来自 Umbrella 控制面板 https://dashboard.umbrella.com 的 OrgInfo.json。
2. 重命名文件 OrgInfo.xml。
3. 按照配置 ISE 以部署 AnyConnect，第 26 页中的步骤操作。

云更新

Umbrella 漫游安全模块可从 Umbrella 云基础设施为所有已安装的 AnyConnect 模块提供自动更新。通过云更新，可自动从 Umbrella 云基础设施获得软件升级，且更新跟踪将取决于该软件升级，而非管理员的任何操作。

默认情况下，将禁用通过云更新进行自动更新。要为 Umbrella 漫游安全和 AnyConnect 的其余模块启用云更新，请登录到 Umbrella 控制面板。在**身份 (Identities) > 漫游计算机 (Roaming Computers)** > 设置图标（齿轮图标）下，选中**无论何时发布新版本，都自动更新 AnyConnect，包括 VPN 模块 (Automatically update AnyConnect, including VPN module, whenever new versions are released)**。更新将在 VPN 处于活动状态时进行。默认情况下，不会选择此选项。

需要考虑以下有关云更新的情况：

- 只会更新当前安装的软件模块。
- 不支持定制、本地化和任何其他部署类型。
- 更新仅在登录到桌面时才会进行，如果建立了 VPN，则不会进行更新。
- 当禁用更新时，最新软件功能和更新将不可用。
- 禁用云更新对其他更新机制或设置（例如网络部署、延迟更新等）没有影响。
- 云更新将忽略装有较新、未发布的版本（例如临时版本和修补版本）AnyConnect 的设备。

配置安全策略以及审核报告

您必须有思科 Umbrella 漫游帐户，才能接受保护、查看报告信息以及配置策略。请访问 https://docs.umbrella.com/product/umbrella/ 以了解深入说明，或请访问 https://support.umbrella.com 以了解更多信息。

在安装后，可在 90 分钟至 2 小时后在您的 Umbrella 控制面板中看到漫游计算机。导航到 https://dashboard.umbrella.com 进行身份验证，然后转到 **Identities > Roaming Computers**，将显示漫游客户端的列表（包括处于活动状态和非活动状态的漫游客户端），以及关于每个已安装客户端的详情。

最初将为您的漫游计算机应用包含基本安全筛选级别的默认策略。此默认策略可在控制面板的Policies部分（或 Configuration > Policy for Cisco Umbrella accounts）中找到。

可在 Policies 部分下找到漫游客户端的报告。选中“活动搜索”(Activity Search) 报告以查看来自装有 Umbrella 漫游安全模块并已关闭 VPN 的计算机的 DNS 流量。

对诊断进行解读

您应运行 DART 报告，以诊断任何思科 Umbrella 漫游安全模块问题。有关 Umbrella 的问题和故障排除详情，请参阅 https://docs.umbrella.com/umbrella-user-guide/docs/appendix-c-troubleshooting。

AnyConnect Umbrella 安全 Web 网关模块

AnyConnect Umbrella Roaming Security 模块提供 DNS 层的安全保护，而 AnyConnect Umbrella Secure Web Gateway (SWG) Agent 模块则在终端上提供了一层安全保护，提高了更多部署场景的灵活性和可能性。Umbrella SWG 允许您在非预期和预期两种情况上安全地对 Web 流量进行身份验证和重定向。此实施需要从 Umbrella 增订 SIG Essentials 或 SIG。

SWG 客户端将加密信头插入 HTTP 请求，头端提取信头，对其进行解密，并使用其用户数据进行身份和策略的确定和实施。同样，对于 HTTPS 流量，SWG 客户端使用 SWG 头端发起 HTTP 连接请求，而连接请求会传输加密报头，这些信头会被提取、解密并用于身份/策略确定和实施。

默认情况下，SWG 在端口 80 和 443 上拦截 HTTP 或 HTTPS 流量。可以使用 Umbrella 云配置添加非标准端口（除 80 和 44 之外）。配置后，除默认标准端口外，SWG 还会在这些额外端口上侦听 HTTP/HTTPS 流量。

通过值得信赖的网络检测，用户可以选择在值得信赖的网络上停用 SWG。在 Umbrella 云中配置此设置后，如果 AnyConnect VPN 隧道处于活动状态，则 SWG 功能将在值得信赖的网络上禁用。“UI 统计信息”(UI Statistics) 窗口中显示的网络保护状态反映了状态的任何更改。

注释 配置此设置后，还会在出现由 Umbrella 的 DNS 保护状态导致的某些错误（例如 Umbrella 解析器无法访问）时停用 SWG。

任何不应代理的域或 IP 地址可在 Umbrella 控制面板的“部署”>“域管理”下定义。不支持通配符，但 Umbrella 将匹配父级域下属的任何子域；例如，如果 example.com 进入域管理列表，则

www.example.com 也将匹配并被跳过。以无类域间路由 (CIDR) 表示法输入 IP 地址。目前仅支持 IPv4 地址。

如果 AnyConnect 无法打开与 Umbrella 代理的连接，则默认情况下 AnyConnect 会打开失败，从而允许直接访问用户。您不能配置这种硬编码行为。

有关这些 Umbrella UI 配置的其他信息，请参阅《思科 Umbrella SIG 用户指南》 。

SWG 的局限性

- 如果安装了 AnyConnect 的本地主机也配置了代理自动配置 (PAC) 文件，PAC 文件优先于 AnyConnect。
- 当前仅支持 IPv4。
- 本地代理不受支持。
- 安装后，Umbrella SWG Agent 可能需要长达 50 分钟的时间与 Umbrella 云同步并接收其配置。不过，默认网络策略应一直应用到同步发生。

Umbrella SWG 的安装和升级

AnyConnect Umbrella SWG 模块仅适用于 Windows 或 macOS，不需要 AnyConnect 核心 (VPN)。但是，如果 AnyConnect 核心 (VPN) 与 AnyConnect Umbrella SWG Agent 一起安装，必须在 VPN 配置文件中启用 *AllowLocalProxyConnections* 设置。

系统支持通过 ASA 或 ISE 进行预部署和 Web 部署。

通过伞云支持云升级。

Umbrella SWG 日志文件和消息

Umbrella 漫游客户端以 SWGConfig.json 文件格式将配置信息发送到 AnyConnect。SWGConfig 的日志文件和消息存储在以下位置：

- Windows—C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\SWG
- macOS-/opt/cisco/anyconnect/umbrella/swg/

漫游安全磁贴中的状态

您可以在“高级统计信息”窗口中验证 SWG 的状态。在该窗口的漫游安全磁贴中，Web 保护状态表示以下其中一项：

- 已禁用 - Umbrella 服务已关闭
- 受保护 — acswgagent 正在运行
- 未受保护 — acswgagent 未运行
- 配置错误 — SWGConfig.json 中的值不正确
- 云服务不可用-无法访问伞代理

有关 Umbrella SWG Agent 的详细统计信息，请打开 AnyConnect UI 并导航到漫游安全分支，以查看重定向到 Umbrella 代理的 HTTP 请求数、重定向到 Umbrella 代理的 HTTPS 请求数、无法重定向到代理的请求数以及 AnyConnect 连接到的 Umbrella 代理。错误和信息性消息记录在邮件历史记录中。

Umbrella SWG 故障排除

如果您在“日志文件选择”(Log File Selection) 窗口中选中“Cisco AnyConnect Umbrella 漫游安全模块”(Cisco AnyConnect Umbrella Roaming Secure Module)，则运行 DART 捆绑包时，它将包括 SWGConfig.json 和 SWG 相关的日志。转到 http://httpbin.org/ip 以检查流量是否到达 Umbrella 代理。如果您遇到连接重置，请发送 HTTP 请求以查看响应代码：

- 如果 HTTP 响应代码为 452，请检查客户端的时钟是否同步或者时间戳是否不正确。恶意用户可能正在尝试重放信头。
- 如果 HTTP 响应代码为 401，则密钥不是最新的。在 "伞控制面板" 上检查设备的上次同步时间。

第 10 章

在本地策略中启用 FIPS

关于 FIPS、NGE 和 AnyConnect

AnyConnect 集成了思科通用加密模块 (C3M)。此思科 SSL 实施在其下一代加密 (NGE) 算法中，包含了符合联邦信息处理标准 (FIPS) 140-2 标准的加密模块和美国国家安全局 (NSA) 套件 B 加密。

NGE 引入新加密、身份验证、数字签名和密钥交换算法，以升级安全和性能需求。RFC 6379 定义了符合美国 FIPS 140-2 标准的套件 B 加密算法。

AnyConnect 组件根据前端、ASA 或 IOS 路由器的配置协商并使用 FIPS 标准加密。以下 AnyConnect 客户端模块支持 FIPS：

- AnyConnect 核心 VPN - 通过在用户计算机上的本地策略文件中使用 FIPS 模式参数，启用符合 FIPS 标准的 VPN 客户端。套件 B 加密适用于 TLS/DTLS 和 IKEv2/IPsec VPN 连接。有关详细信息和过程，请参阅为 AnyConnect 核心 VPN 客户端配置 FIPS。

  除 FIPS 模式以外，AnyConnect 本地策略文件 AnyConnectLocalPolicy.xml 还包含适用于本地客户端的其他安全设置。此文件并未通过 ASA 进行部署，且必须手动安装，或使用企业软件部署系统进行部署。有关使用此配置文件的详细信息，请参阅 AnyConnect 本地策略。

- AnyConnect 网络访问管理器 - 通过在 AnyConnectLocalPolicy.xml 文件中使用 FIPS 模式参数和在网络访问管理器配置文件中使用 FIPS 模式参数，启用符合 FIPS 标准的网络访问管理器。Windows 中支持用于网络访问管理器的 FIPS。有关详细信息和步骤，请参阅为网络访问管理器配置 FIPS。

AnyConnect 中的 FIPS 功能

功能	核心 VPN 模块	网络访问管理器模块
对称加密和完整性的 AES-GCM 支持。	用于 IKEv2 负载加密和身份验证的 128 位、192 位和 256 位密钥。 ESP 数据包加密和身份验证。	软件中有线流量加密的 802.1AE (MACsec) 的 128 位密钥 (Windows)。
哈希值算法的 SHA-2 支持，采用 256/384/512 位的 SHA。	IKEv2 负载身份验证和 ESP 数据包身份验证。（Windows 7 或更高版本和 macOS 10.7 或更高版本）。	能够在基于 TLS 的 EAP 方法中使用 SHA-2 证书。
密钥交换的 ECDH 支持。	组 19、20 和 21 IKEv2 密钥交换及 IKEv2 PFS。	能够在基于 TLS 的 EAP 方法中使用 ECDH (Windows)。
数字签名、不对称加密和身份验证的 ECDSA 支持，即 256 位、384 位、521 位椭圆曲线。	IKEv2 用户身份验证和服务器证书验证。	能够在基于 TLS 的 EAP 方法中使用 ECDSA 证书。
其他支持	IPsecV3 的所有必需加密算法（NULL 加密除外）。 TLS/DTLS 和 IKEv2 的 4096 位密钥 RSA 证书。	不适用

[1] 在 Linux 中，对 ECDSA 仅支持 AnyConnect 文件存储。要向文件存储库添加证书，请参阅为 macOS 和 Linux 创建 PEM 证书存储库。

[2] IPsecV3 还规定必须支持扩展序列号 (ESN)，但 AnyConnect 不支持 ESN。

AnyConnect FIPS 要求

- 套件 B 加密适用于 TLS/DTLS 和 IKEv2/IPsec VPN 连接。
- 安全网关中需要 FIPS 和/或套件 B 支持。思科在 ASA 9.0 版及更高版本中提供套件 B 功能，在 ASA 8.4.1 版及更高版本中提供 FIPS 功能。
- ECDSA 证书要求：
  - 摘要强度必须大于或等于曲线强度。例如，EC-384 密钥必须使用 SHA2-384 或更高版本。
  - 支持的操作系统：Windows 7 或更高版本、macOS 10.7 或更高版本、Red Hat Enterprise Linux 6.x 或 6.4（64 位），以及 Ubuntu 12.4 和 12.10（64 位）。ECDSA 智能卡仅在 Windows 7（和更高版本）中受支持。

AnyConnect FIPS 的限制

在验证使用 SHA-2 签署的证书时，除了在基于 TLS 的 EAP 中，没有 EAP 方法支持 SHA-2。

AnyConnect FIPS 指南

- AnyConnect 客户端的 Statistics 面板（在 Transport Information 标题下）显示正在使用的密码名称。
- 由于 AES-GCM 是计算密集型的算法，因此使用这些算法时您可能会体验到整体数据速率降低。部分新 Intel 处理器包含专门引进以提升 AES-GCM 性能的特别说明。AnyConnect 会自动检测正在运行的处理器是否支持这些新指令。若支持，AnyConnect 将使用新指令，从而相对于那些没有特殊指令的处理器来说，可以显著提高 VPN 数据速率。请参阅 http://ark.intel.com/Search/FeatureFilter?productType=processors&AESTech=true 了解支持新指令的处理器列表。有关详细信息，请参阅 http://software.intel.com/en-us/articles/intel-carry-less-multiplication-instruction-and-its-usage-for-computing-the-gcm-mode/。
- 组合模式加密算法（它在一次操作中同时执行加密和完整性验证）仅在具有硬件加密加速的 SMP ASA 网关（例如 5585 和 5515-X）上受支持。AES-GCM 是思科支持的组合模式加密算法。

  注释 IKEv2 策略既可以包含普通模式加密算法，也可以包含组合模式加密算法，但不能同时包含这两种类型。当组合模式算法配置在 IKEv2 策略中时，所有普通模式算法都被禁用，因此唯一有效的完整性算法为 NULL。

  IKEv2 IPsec 提议使用其他模型，可以在同一提议中同时指定普通模式和组合模式加密算法。对于这种用法，您需要为这两种算法都配置完整性算法，给 AES-GCM 加密算法配置的是非 NULL 完整性算法。
- 当 ASA 配置为对 SSL 和 IPsec 使用不同的服务器证书时，请使用受信任证书。如果使用具有不同 IPsec 和 SSL 证书的套件 B (ECDSA) 不受信任证书，则状态评估、WebLaunch 或下载程序可能发生故障。

避免因 AnyConnect FIPS 注册表更改导致的终端问题

为核心 AnyConnect 客户端启用 FIPS 会更改终端上的 Windows 注册表设置。终端的其他组件可能会检测到 AnyConnect 已启用 FIPS 并开始使用加密。例如，Microsoft 终端服务客户端远程桌面协议 (RDP) 将不工作，因为 RDP 要求服务器使用符合 FIPS 的加密。

为避免这些问题，您可以通过将参数 Use FIPS compliant algorithms for encryption, hashing, and signing 更改为 Disabled，在 Windows Local System Cryptography 设置中临时禁用 FIPS 加密。请注意重启终端设备将此设置改回已启用。

AnyConnect 将 Windows 注册表项 HKLM\System\CurrentControlSet\Control\Lsa 中的 FIPSAlgorithmPolicy 值设置为 1。请注意，在 AnyConnect 本地策略文件中禁用 FIPS 模式不会导致 AnyConnect 更改 FIPSAlgorithmPolicy 值。

为 AnyConnect 核心 VPN 客户端配置 FIPS

为 AnyConnect 核心 VPN 启用 FIPS

步骤 1 在 AnyConnect 配置文件编辑器中打开或创建一个 VPN 本地策略配置文件。

步骤 2 选择**FIPS 模式 (FIPS Mode)**。

步骤 3 保存此 VPN 本地策略配置文件。

我们建议您对此配置文件进行命名来表示已启用 FIPS。

在 Windows 安装期间启用 FIPS

对于 Windows 安装，您可以将 Cisco MST 文件应用于标准 MSI 安装文件，以便在 AnyConnect 本地策略中启用 FIPS。有关此 MST 文件的下载位置的信息，请参阅您收到的 FIPS 的许可信息。安装期间将生成已启用 FIPS 的 AnyConnect 本地策略文件。在运行此实用程序后，更新用户系统。

注释 此 MST 只启用 FIPS。它不会更改其他参数。要在 Windows 安装期间更改其他本地策略设置，请参阅在 MST 文件中启用本地策略参数。

为网络访问管理器配置 FIPS

网络访问管理器可配置为同时连接到 FIPS 和非 FIPS 网络，或者只连接到 FIPS 网络。

SUMMARY STEPS

1. 为网络访问管理器启用 FIPS。
2. 如果需要，请参阅为网络访问管理器实施 FIPS 模式。

DETAILED STEPS

步骤 1 为网络访问管理器启用 FIPS。

启用 FIPS 可允许网络访问管理器同时连接到 FIPS 和非 FIPS 网络。

步骤 2 如果需要，请参阅为网络访问管理器实施 FIPS 模式。

实施 FIPS 模式会将网络访问管理器连接仅限于 FIPS 网络。

为网络访问管理器启用 FIPS

在 AnyConnect 网络访问管理器客户端配置文件中启用 FIPS 模式：

a) 在 AnyConnect 配置文件编辑器中打开或创建一个网络访问管理器配置文件。
b) 选择**客户端策略 (Client Policy)** 配置窗口。
c) 在**管理状态 (Administrative Status)** 部分下，为 **FIPS 模式 (FIPS Mode)** 选择 **启用 (Enable)**。
d) 将网络访问管理器配置文件另存为 configuration.xml。

为网络访问管理器实施 FIPS 模式

通过在网络访问管理器配置文件中限制允许的关联和加密模式以及身份验证方法，强制企业员工只连接到符合 FIPS 的网络。

必须首先为网络访问管理器启用 FIPS 以强制实施 FIPS 模式。

步骤 1 在 AnyConnect 配置文件编辑器中打开网络访问管理器配置文件。

步骤 2 网络访问管理器 FIPS 合规性要求 FIPS 批准的 AES 加密模式，包括 WPA2 个人模式 (WPA2-PSK) 和 WPA2 企业模式 (802.1X)。

步骤 3 网络访问管理器 FIPS 支持 EAP 方法，包括 EAP-TLS、EAP-TTLS、PEAP、EAP-FAST 和 LEAP。

步骤 4 将网络访问管理器配置文件另存为 configuration.xml。

第 11 章

移动设备上的 AnyConnect

移动设备上的 AnyConnect 类似于 Windows、macOS 和 Linux 平台上的 AnyConnect。本章介绍设备信息、配置信息、支持信息，以及适用于移动设备的 AnyConnect 特定的其他管理任务。

移动设备上的 AnyConnect 操作和选项

关于 AnyConnect 移动 VPN 连接

此版本的 AnyConnect 安全移动客户端可用于以下移动平台：

- Android
- Apple iOS
- Chromebook
- Windows Phone

每个受支持平台的应用商店都提供了思科 AnyConnect。它在 www.cisco.com 上不可用，或无法从安全网关进行分发。

AnyConnect 移动应用仅包含核心 VPN 客户端。它们不包括网络访问管理器或终端安全评估等其他 AnyConnect 模块。在连接 VPN 的状态下，此应用使用 AnyConnect Identify Extensions (ACIDex) 向前端提供终端安全评估信息（称为“移动终端安全评估”）。

AnyConnect VPN 连接可以通过以下方法之一建立：

- 用户手动建立。
- 用户在单击管理员提供的自动连接操作时手动建立（仅适用于 Android 和 Apple iOS）。
- 通过按需连接功能自动建立（仅适用于 Apple iOS）。

移动设备上的 AnyConnect VPN 连接条目

连接条目通过安全网关的完全限定域名或 IP 地址（如有需要，包括隧道组 URL）识别安全网关地址。该连接条目还可以包括其他连接属性。

AnyConnect 支持在一个移动设备上拥有多个连接条目，以便寻址不同安全网关和/或 VPN 隧道组。如果配置了多个连接条目，则用户应了解使用哪个条目来发起VPN连接。通过以下方法之一来配置连接条目：

- 用户手动配置。有关在移动设备上配置连接条目的过程，请参阅相应平台的用户指南。
- 连接条目将在用户单击管理员提供的用于配置连接条目的链接后添加。

  请参阅生成 VPN 连接条目，第 274 页可向用户提供此类连接条目配置。
- 由 Anyconnect VPN 客户端配置文件定义。

  AnyConnect VPN 客户端配置文件指定客户端行为并定义 VPN 连接条目。有关详细信息，请参阅在 AnyConnect VPN 配置文件中配置移动设备连接，第 272 页。

隧道型号

AnyConnect 可以在托管或未托管的自带设备 (BYOD) 环境中运行。这些环境中的 VPN 隧道只在以下一种型号中运行：

- 系统隧道型号 - VPN 连接用于传送所有数据（全隧道），或仅传送流入/流出特定域或地址的数据（分割隧道）。此型号可在所有移动平台上使用。
- Per App VPN 模式 - VPN 连接用于移动设备上的特定应用集（仅限 Android 和 Apple iOS）。

  AnyConnect 允许管理员在前端上定义一组应用。此列表使用 ASA 自定义属性机制来定义。此列表将发送给 AnyConnect 客户端，并在设备上实施。对于所有其他应用，在隧道之外或以明文形式发送数据。

  在 Apple iOS 上，需要有受管环境才能在此型号下运行。在 Android 上，受管和非受管环境均受支持。在这两个平台上的托管环境中，移动设备管理器还必须将设备配置为传送与 AnyConnect 配置传送相同的应用列表。
- 多隧道 - iOS 上的 AnyConnect 支持以下模式的多个隧道：

- 一次连接一个常规（非 Per App）VPN 隧道和一个或多个 Per App 隧道
- 一次连接多个 Per App VPN 隧道

请参阅适用于 iOS 的多隧道，第 245 页获得更多信息。

AnyConnect 的运行型号由从 ASA 前端收到的配置信息决定。特别是，与连接相关的组策略或动态访问策略 (DAP) 中是否存在 Per App VPN 列表。如果 Per App VPN 列表存在，AnyConnect 会在 Per App VPN 型号下运行；如果列表不存在，AnyConnect 会在系统隧道连接型号下运行。

适用于 iOS 的多隧道

AnyConnect 用户只能手动启动一个隧道的 VPN 连接（无论是否有 Per-App VPN）。由于 Per-App VPN 自动从关联的应用开始，因此您必须在 MDM VPN 配置文件的 VendorConfig 中添加 **MultiTunnel** 密钥并将其设置为 **true**，才能使用多隧道。

在 iOS AnyConnect 主页屏幕中，您将看到一个显示所选隧道（无论是否已连接）的表。第二个表是动态的，仅在连接 Per-App VPN 时才显示。第二个表只显示 Per-App 隧道的连接状态，直到用户单击**状态 (Status)** 才能查看已接收和发送字节的连接的详细统计信息。

您可以参阅“诊断”，查看当前选定的常规 VPN 日志。当用户决定共享日志时，日志包会包含连接的 VPN 配置的所有 VPN 调试日志文件。

移动设备的安全网关身份验证

阻止不受信任的服务器

建立 VPN 连接时，AnyConnect 将使用从安全网关接收的数字证书来验证服务器的身份。如果服务器证书无效（因过期或日期无效、密钥使用错误或名称不匹配导致证书错误），或证书不受信任（证书无法由证书颁发机构验证），抑或同时出现上述两种情况，则连接将被阻止。此时将显示一条阻止消息，用户必须选择如何处理。

阻止不受信任的服务器 (Block Untrusted Servers) 应用设置确定 AnyConnect 在无法识别安全网关时的响应方式。默认情况下开启此保护；用户可关闭此保护，但不建议这样做。

当**阻止不受信任的服务器 (Block Untrusted Servers)** 开启后，将向用户显示一条**不受信任的 VPN 服务器 (Untrusted VPN Server)** 阻止通知，告知此安全威胁。用户可选择：

- **保持我的安全状态 (Keep Me Safe)** 以终止此连接，保持安全。
- **更改设置 (Change Settings)** 以关闭“阻止不受信任的服务器”(Block Untrusted Servers) 应用首选项，但不建议这样做。用户禁用此安全保护功能后，必须重新初始化 VPN 连接。

当**阻止不受信任的服务器 (Block Untrusted Servers)** 关闭后，将向用户显示一条**不受信任的 VPN 服务器 (Untrusted VPN Server)** 取消阻止通知，告知此安全威胁。用户可选择：

- **取消 (Cancel)** 以取消连接并保持安全。
- **继续 (Continue)** 以继续连接，但不建议这样做。

- **查看详细信息 (View Details)** 以查看证书详细信息，更直观地判断证书的可接受性。

  如果用户正在查看的证书有效但不受信任，则用户可以：

  - 选择**导入并继续 (Import and Continue)** 将服务器证书导入 AnyConnect 证书存储区供以后使用，并继续连接。

    当此证书导入 AnyConnect 存储区后，使用此数字证书与服务器建立的后续连接将被自动接受。

  - 返回上一屏幕并选择**取消 (Cancel)** 或**继续 (Continue)**。

  如果证书因任何原因无效，用户只能返回上一屏幕并选择**取消 (Cancel)** 或**继续 (Continue)**。

最安全的网络 VPN 连接配置是：开启“阻止不受信任的服务器”(Block Untrusted Servers) 设置（默认设置），在安全网关上配置有效且受信任的服务器证书，并指示移动用户始终选择“保持我的安全状态”(Keep Me Safe)。

注释 **严格证书信任**将覆盖此设置，请参阅以下说明。

OCSP 吊销

AnyConnect 客户端支持 OCSP（在线证书状态协议）。由此，使客户端可以实时查询各个证书的状态，具体方法为：向 OCSP 响应程序发送请求，并解析 OCSP 响应，即可获得证书状况。OCSP 用于验证整个证书链。对于每个证书，访问 OCSP 响应程序设有五秒的超时间隔。

用户可以在 Anyconnect 设置活动中启用或禁用 OCSP 验证，详细信息请参阅Cisco AnyConnect Secure Mobility Client 用户指南 (Android)，版本 4.6。此外，我们还在框架中添加了新 API 验证，MDM 管理员可使用其远程控制此功能。目前支持 Samsung 和 Google MDM。

严格证书信任

如果用户启用此项，在验证远程安全网关时，AnyConnect 将禁用任何无法验证的证书。客户端会连接安全网关失败，而不是提示用户接受这些证书。

注释 此设置将覆盖 **阻止不受信任的服务器**。

如果未选中，客户端将提示用户接受证书。这是默认行为。

我们强烈建议您为 AnyConnect 客户端启用“严格证书信任”，原因如下：

- 随着有针对性攻击的日益增多，在本地策略中启用 Strict Certificate Turst 有助于在用户从不受信任网络（例如公共访问网络）连接时，防止受到“中间人”攻击。
- 即使您使用完全可验证且受信任的证书，默认情况下 AnyConnect 客户端也允许最终用户接受不可验证的证书。如果最终用户受到中间人攻击，他们可能会被提示接受恶意证书。要从最终用户删除此决定，请启用 Strict Certificate Turst。

移动设备上的客户端身份验证

要完成VPN连接，用户必须提供用户名和密码、数字证书或这两种形式的凭证进行身份验证。管理员可以定义隧道组上的身份验证方法。为了保证在移动设备上提供最佳用户体验，思科建议根据身份验证配置情况使用多个AnyConnect连接配置文件。您必须确定平衡用户体验和安全的最佳方法。我们的建议如下：

- 对于移动设备的基于 AAA 的身份验证隧道组，组策略应有很长的空闲超时（例如 24 小时），以让客户端在无需用户重新进行身份验证的情况下即可保持重新连接状态。
- 要实现最透明的最终用户体验，请仅使用证书进行身份验证。使用数字证书时，无需用户交互即可建立 VPN 连接。

为了使用证书对连接安全网关的移动设备进行身份验证，最终用户必须在其设备上导入证书。之后，此证书可用于自动证书选择，也可以手动将其与特定连接条目关联。可使用以下方法导入证书：

- 由用户手动导入。有关向移动设备导入证书的过程，请参阅相关的用户指南。
- 使用 SCEP。有关详细信息，请参阅配置证书注册，第 146 页。
- 在用户单击管理员提供的链接以导入证书之后，便会添加。

  请参阅导入证书，第 280 页为您的用户提供这种证书部署。

在移动设备上本地化

适用于 Android 和 Apple iOS 的 AnyConnect 安全移动客户端支持本地化，可根据用户的区域设置调整 AnyConnect 用户界面和消息。

预包装的本地化

AnyConnect 和 Apple iOS 应用包括以下语言翻译：

- 加拿大法语 (fr-ca)
- 中文（台湾地区）(zh-tw)
- 捷克语 (cs-cz)
- 荷兰语 (nl-nl)
- 法语 (fr-fr)
- 德语 (de-de)
- 匈牙利语 (hu-hu)
- 意大利语 (it-it)
- 日语 (ja-jp)
- 韩语 (ko-kr)

- 拉丁美洲西班牙语 (es-co)
- 波兰语 (pl-pl)
- 葡萄牙语（巴西）(pt-br)
- 俄语 (ru-ru)
- 简体中文 (zh-cn)
- 西班牙语 (es-es)

安装 AnyConnect 时，这些语言的本地化数据会安装到移动设备上。移动设备上指定的本地化设置决定显示的语言。AnyConnect 会依次使用语言规范和地区规范来确定最佳匹配设置。例如，安装完成后，在法语-瑞士 (fr-ch) 区域设置下，最终的显示为法语-加拿大 (fr-ca)。AnyConnect 启动后，AnyConnect 用户界面和消息会被翻译为本地语言。

下载的本地化

对于不在 AnyConnect 软件包中的语言，管理员向 ASA 添加要通过 AnyConnect VPN 连接下载到设备的本地化数据。

思科在 Cisco.com 的产品下载中心提供 anyconnect.po 文件，其中包括所有可本地化的 AnyConnect 字符串。AnyConnect 管理员可下载 anyconnect.po 文件，提供可用字符串的翻译，然后将文件上传到 ASA。已将 anyconnect.po 文件安装到 ASA 上的 AnyConnect 管理员可下载此更新版本。

最初，AnyConnect 用户界面和消息以安装语言向用户显示。在设备用户建立了与 ASA 的第一个连接后，AnyConnect 将比较设备的首选语言与 ASA 上的可用本地化语言。如果 AnyConnect 找到匹配的本地化文件，则下载该本地化文件。下载完成后，AnyConnect 将使用已添加到 anyconnect.po 文件的翻译字符串显示用户界面和用户消息。如果字符串未翻译，AnyConnect 将显示默认的英语字符串。

有关在 ASA 上配置本地化的说明，请参阅将转换表导入自适应安全设备，第 52 页。如果 ASA 不包含设备区域设置的本地化数据，将继续使用 AnyConnect 应用软件包中预装的本地化数据。

在移动设备上提供本地化的更多方式

本地化 AnyConnect 用户界面和消息，第 281 页可为用户提供 URI 链接。

要求移动设备用户在自己的设备上管理本地化数据。有关执行以下本地化活动的程序，请参阅相应的用户指南：

- 从指定服务器导入本地化数据。用户选择导入本地化数据并指定安全网关的地址和区域设置。根据 ISO 639-1 指定区域设置，如适用，可添加国家代码（例如，en-US、fr-CA、ar-IQ 等等）。此本地化数据用来替代预先打包的已安装本地化数据。
- 恢复默认的本地化数据。此操作将恢复使用 AnyConnect 软件包中预装的本地化数据，并删除已导入的所有本地化数据。

使用 SAML 进行 VPN 身份验证

在下列版本中，SAML 2.0 支持已被添加到移动设备。使用 SAML 身份验证时，它仅适用于 AnyConnect 会话。它不适用于网站，浏览器启动的 SAML 登录或已安装的应用程序。为了提供无中断的无缝重新连接，AnyConnect 将故意跳过重复的 SAML 身份验证过程。此外，如果用户使用浏览器从 IdP 注销，AnyConnect 会话仍将保持不变。

- iOS - 版本 4.6； SAML 加上客户端证书（版本 4.8）
- Android - 版本 4.6；SAML 加上客户端证书（版本 4.8）
- Chrome - 版本 4.0

在使用 SAML 时，请遵循以下指导原则：

- 如果在故障转移型号下使用永远在线 VPN，则不支持外部 SAML IdP（但是，使用内部 SAML IdP，ASA 会代理到 IdP 的所有流量并且受支持）
- 在嵌入式浏览器中不允许不受信任的服务器证书。
- CLI 或 SBL 型号中不支持嵌入式浏览器 SAML 集成。
- （仅移动设备）不支持单一注销。
- 在网络浏览器中建立的 SAML 身份验证不会与 AnyConnect 共享，反之亦然。
- 根据具体配置，在使用嵌入式浏览器连接到前端时，会使用各种不同的方法。例如，尽管 AnyConnect 相比于 IPv6 连接更喜欢 IPv4 连接，但嵌入式浏览器可能更喜欢 IPv6，或反之亦然。同样，在尝试代理和收到失败后，AnyConnect 可能会回退到没有代理状态，而嵌入式浏览器在尝试代理并收到失败后可能会停止导航。
- 为了使用 SAML 功能，必须使您的 ASA 网络时间协议 (NTP) 服务器与 IdP NTP 服务器同步。
- ASDM 上的 VPN 向导目前不支持 SAML 配置。
- SAML IdP *NameID* 属性确定用户的用户名，并且用于授权、记帐和 VPN 会话数据库。
- 如果您希望用户每次通过 SAML 建立 VPN 会话时，都使用身份提供程序 (IdP) 重新进行身份验证，则应该在 AnyConnect 配置文件编辑器，首选项（第 1 部分），第 74 页中将 Auto Reconnect 设置为 *ReconnectAfterResume*。
- 由于具有嵌入式浏览器的 AnyConnect 会针对每个 VPN 尝试使用新的浏览器会话，因此，如果 IdP 使用 HTTP 会话 cookie 来跟踪登录状态，则用户每次都必须重新进行身份验证。这种情况下，**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 无客户端 SSL VPN 访问 (Clientless SSL VPN Access) > 高级 (Advanced) > 单点登录服务器 (Single Sign On Servers)** > 中的强制重新验证 *(Force Re-Authentication)* 设置对 AnyConnect 启动的 SAML 身份验证没有任何影响。

有关其他配置详细信息，请参阅相应版本（9.7 或更高版本）的思科 ASA 系列 VPN 配置指南中的使用 *SAML 2.0* 的 *SSO* 部分。

将转换表导入自适应安全设备

步骤 1 从 www.cisco.com 下载所需的转换表。

步骤 2 在 ASDM 中，转到 **配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **AnyConnect 定制/本地化 (AnyConnect Customization/Localization)** > **GUI 文本和消息 (GUI Text and Messages)**。

步骤 3 单击**导入 (Import)**。系统会显示“导入语言本地化条目”(Import Language Localization Entry) 窗口。

步骤 4 从下拉列表中选择适合的语言。

步骤 5 指定从何处导入转换表。

步骤 6 单击**立即导入 (Import Now)**。即可将此转换表部署至 AnyConnect 客户端，并将其用作首选语言。本地化将在 AnyConnect 重新启动并连接后应用。

注释 对于在非移动设备上运行的 AnyConnect，即使没有使用思科安全桌面，也必须将思科安全桌面转换表导入自适应安全设备，这样 HostScan 消息才会进行本地化。

移动设备上的 FIPS 和套件 B 加密

用于移动设备的 AnyConnect 包含思科通用加密模块 (C3M)，该 Cisco SSL 实现包括 FIPS 140-2 兼容的加密模块和 NSA 套件 B 加密，是下一代加密 (NGE) 算法的一部分。套件 B 加密仅适用于 IPsec VPN；FIPS 兼容加密同时适用于 IPsec 和 SSL VPN。

连接时与前端协商加密算法的使用。协商取决于VPN连接两端的功能。因此，安全网关还必须支持 FIPS 兼容加密和套件 B 加密。

用户可将 AnyConnect 配置为仅在协商期间接受 NGE 算法，方法是在 AnyConnect 应用设置中启用 **FIPS 型号 (FIPS Mode)**。当“FIPS 型号”(FIPS Mode) 处于禁用状态时，AnyConnect 也接受 VPN 连接使用非 FIPS 加密算法。

其他移动准则和限制

- 套件 B 加密要求 Apple iOS 5.0 或更高版本；这是支持套件 B 中使用的 ECDSA 证书的 Apple iOS 最低版本。
- 套件 B 加密要求 Android 4.0 (Ice Cream Sandwich) 或更高版本；这是支持套件 B 中使用的 ECDSA 证书的 Android 最低版本。
- 在 FIPS 型号下运行的设备与按代理方法或传统方法使用 SCEP 为移动用户提供数字证书的方式不兼容。请相应计划您的部署。

Android 设备上的 AnyConnect

有关该版本的功能和更新，请参阅适用于 Android 的 Cisco AnyConnect Secure Mobility Client 4.x 版发行说明。

有关此版本支持的功能和设备，请参阅 AnyConnect 移动平台和功能指南。

Android 版 AnyConnect 的准则和限制

- ASA 不对 Android 版 AnyConnect 提供分发和更新。它们仅在 Google Play 中提供。最新版本的 APK（软件包）文件也发布在 Cisco.com 上。
- Android 版 AnyConnect 仅支持 Network Visibility Module 和 Umbrella，不支持任何其他 AnyConnect 模块。
- Android 设备仅支持一个 AnyConnect 配置文件，即，从前端接收的最后一个配置文件。但是，一个配置文件可能包含多个连接条目。
- 如果用户尝试在不受支持的设备上安装 AnyConnect，将收到弹出消息安装错误：原因未知 -8 (Installation Error: Unknown reason -8)。此消息由 Android OS 生成。
- 如果用户在其主屏幕上安装 AnyConnect 构件，那么，无论是否选择了“在启动时启动”(Launch at startup) 首选项，AnyConnect 服务都将自动启动（但不连接）。
- 使用“从客户端证书预填充”功能时，Android 版 AnyConnect 需要对扩展的 ASCII 字符进行 UTF-8 字符编码。根据 KB-890772 和 KB-888180 中的说明，如果您想使用预填充，客户端证书必须采用 UTF-8 格式。
- AnyConnect 在通过 EDGE 连接发送或接收 VPN 流量时会阻止语音呼叫，这是 EDGE 和其他早期无线电技术的固有性质所决定的。
- 一些已知的文件压缩实用程序无法成功解压缩使用 AnyConnect“发送日志”(Send Log) 按钮打包的日志捆绑包。其解决方法是使用 Windows 和 mac OS X 上的本地实用程序解压缩 AnyConnect 日志文件。
- DHE 兼容性 — 在 AnyConnect 版本4.6 中引入 DHE 密码支持后，会导致 ASA 9.2 之前的 ASA 版本出现不兼容问题。如果您使用 ASA 9.2 之前的版本的 DHE 密码，则必须在这些 ASA 版本上禁用 DHE 密码。

Android 特定注意事项

Android 移动终端安全评估设备 ID 生成

现在，AnyConnect 会在全新安装时或用户清除应用数据后，生成基于 Android ID 的 256 字节唯一设备 ID。此 ID 取代基于早期版本中生成的 IMEI 和 MAC 地址的传统 40 字节设备 ID。

如果安装了早期版本的 AnyConnect，则已生成传统 ID。在升级到此版本的 AnyConnect 之后，此传统 ID 继续被报告为设备唯一 ID，直到用户清除应用数据或卸载 AnyConnect。

可通过以下三种方式查看生成的设备 ID：从 AnyConnect **诊断 (Diagnostics)** > **日志记录和系统信息 (Logging and System Information)** > **系统 (System)** > **设备标识符 (Device Identifiers)** 屏幕（在初始应用启动后），在 `device_identifiers.txt` 文件中的 AnyConnect 日志内，或者在**关于 (About)** 屏幕上。

注释 需要更新安全网关上的 DAP 策略，才能使用新设备 ID。

`Device-ID` 的确定方式如下：

```
Device-ID = bytesToHexString(SHA256(Android-ID))
```

其中 `Android-ID` 和 `bytesToHexString` 按如下方式定义：

```
Android-ID = Secure.getString(context.getContentResolver(), Secure.ANDROID_ID)
```

```
String bytesToHexString(byte[] sha256rawbytes){
String hashHex = null;
if (sha256rawbytes != null){
  StringBuffer sb = new StringBuffer(sha256rawbytes.length * 2);
    for (int i = 0; i < sha256rawbytes.length; i++){
    String s = Integer.toHexString(0xFF & sha256rawbytes[i]).toUpperCase();
    if (s.length() < 2) {sb.append("0");}
    sb.append(s);
    }
  hashHex = sb.toString();
  }
return hashHex; }
```

Android 设备权限

适用于 AnyConnect 操作的 Android 清单中声明了以下权限：

清单权限	说明
uses-permission: android.permission.ACCESS_NETWORK_STATE	允许应用访问网络的相关信息。
uses-permission: android.permission.ACCESS_WIFI_STATE	允许应用访问 Wi-Fi 网络的相关信息。
uses-permission: android.permission.BROADCAST_STICKY	允许应用广播粘性意图。这些广播在完成后，其数据由系统保留，以便客户端可以快速检索这些数据，而不必等待下一次广播。
uses-permission: android.permission.INTERNET	允许应用打开网络套接字。
uses-permission: android.permission.READ_EXTERNAL_STORAGE	允许应用从外部存储中读取。
uses-permission: android.permission.READ_LOGS	允许应用读取低层系统日志文件。

清单权限	说明
uses-permission: android.permission.READ_PHONE_STATE	允许只读访问电话状态，包括设备的电话号码、当前的蜂窝网络信息、正在进行的任何呼叫的状态，设备上注册的任何电话帐户列表。
uses-permission: android.permission.RECEIVE_BOOT_COMPLETED	允许应用在系统完成启动后接收广播。

在 Chromebook 上配置 Android 版 AnyConnect

Google 最近宣布弃用所有本地 Chromebook 应用。本文档旨在帮助您从本地 Chromebook 应用迁移，并帮助您在 Chromebooks 上配置 Android 版 AnyConnect。

有关其他信息，您可以访问此 Google 文档。

步骤 1 使用管理员帐户登录 Google 管理员控制台。

步骤 2 在 Google 管理员控制台主页上，转到**设备 > Chrome**。

步骤 3 单击**应用和扩展程序 (Apps & entensions) > 用户和浏览器 (Users & browsers)**。

步骤 4 如果要将设置应用于所有人，请保留顶层组织单位的选中状态。否则，应用子组织单位。

步骤 5 单击**添加 (Add) > 从 Google Play 添加 (Add from Google Play)**。

步骤 6 选择 AnyConnect 作为要管理的应用。

步骤 7 唯一的托管配置是 JSON 文件，您可以通过单击上传图标将其粘贴或上传。

下一步做什么

密钥在 Android 的 .apk 软件包文件中定义。唯一必填字段为 vpn_connection_host，但如果推送的是 AnyConnect XML 配置文件，则 JSON 密钥为 vpn_connection_profile。AnyConnect 支持下一节中列出的所有托管的配置密钥。

AnyConnect 支持的托管配置密钥

受管限制（根）

vpn_connection_name

- 标题 - 连接名称
- 类型 - 字符串
- 说明 - 用户友好名称（仅用于显示）。如果未设置，则默认为 host。

vpn_connection_host

- 标题 - 主机
- 类型 - 字符串

- 说明 - 指向前端的 URL。此栏必填。

vpn_connection_profile

- 标题 - 协议
- 类型 - 选项
- 可能值 - SSL | IPsec
- 说明 - VPN 隧道协议（SSL 或 IPsec）。默认为 SSL

vpn_connection_ipsec_auth_mode

- 标题 - IPsec 身份验证模式
- 类型 - 选项
- 说明 -（可选）当隧道协议为 IPsec 时使用的身份验证模式。默认为 EAP-AnyConnect

vpn_connection_ipsec_ike_identity

- 标题 - IKE 身份
- 类型 - 字符串
- 说明 -（可选）仅当 IPsec 身份验证模式为 EAP_GTC、EAP-Md5 或 EAP-MSCHAPv2 时适用

vpn_connection_ipsec_ike_identity

- 标题 - IKE 身份
- 类型 - 字符串
- 说明 -（可选）仅当 IPsec 身份验证模式为 EAP_GTC、EAP-MD5 或 EAP-MSCHAPv2 时适用。

vpn_connection_keychain_cert_alias

- 标题 - 密钥链证书别名
- 类型 - 字符串
- 说明 -（可选）要用于此 VPN 配置的客户端证书的密钥链别名

vpn_connection_perapp

- 标题 - Per App VPN 允许的应用
- 类型 - 字符串
- 说明 -（已弃用）请使用 vpn_connection_allowed_apps。

vpn_connection_allowed_apps

- 标题 - Per App VPN 允许的应用
- 类型 - 字符串

- 说明 -（可选）指定哪些应用（Android 应用软件包名称的逗号分隔列表）应建立隧道，从而启用 Per App VPN。所有其他应用都不建立隧道。此设置要求在前端上启用 Per App VPN。

vpn_connection_disallowed_apps

- 标题 - Per App VPN 禁止的应用
- 类型 - 字符串
- 说明 -（可选）指定哪些应用（Android 应用软件包名称的逗号分隔列表）不应建立隧道，从而启用 Per App VPN。所有其他应用都建立隧道。此设置要求在前端上启用 Per App VPN。

vpn_connection_allow_bypass

- 标题 - 允许应用绕过 VPN 隧道
- 类型 - bool
- 说明 -（可选）允许应用绕过此 VPN 连接。默认情况下，此项为禁用状态。

vpn_setting_replace_existing_profile

- 标题 - 替换现有配置文件
- 类型 - bool
- 说明 -（可选）仅当设置了 vpn_connection_profile 时适用。指定托管配置的配置文件是否应替换客户端上已安装的任何配置文件。为避免与 ASA 推送的配置文件冲突，可能需要禁用此项。默认情况下，此项为启用状态。

vpn_setting_apply_perapp_to_profile

- 标题 - 对配置文件导入的配置应用 Per App 规则
- 类型 - bool
- 说明 -（可选）指定是否将受管配置 Per-App VPN 规则（如果存在）应用于从 AnyConnect 配置文件 XML 导入的配置。默认情况下，此项为禁用状态。

vpn_connection_set_active

- 标题 - 设置为活动状态
- 类型 - bool
- 默认值 - true
- 说明 -（可选）将此设置为最后一个选择的 VPN 配置（如果没有任何配置）。

vpn_setting_fips_mode

- 标题 - FIPS 模式
- 类型 - bool
- 说明 -（可选）是否为 AnyConnect 启用 FIPS 模式。

vpn_setting_uri_external_control

- 标题 - URI 外部控制
- 类型 - 字符串
- 说明 -（可选）配置 URI 处理（外部控制）。有效选项为“已提示”、“已启用”和“已禁用”。

vpn_setting_strict_mode

- 标题 - 严格模式
- 类型 - bool
- 说明 -（可选）是否为 AnyConnect 启用严格证书信任模式。

vpn_setting_certificate_revocation

- 标题 - 证书撤销
- 类型 - bool
- 说明 -（可选）是否为 AnyConnect 启用 OCSP 服务器证书检查。

vpn_connection_profile

- 标题 - AnyConnect 配置文件
- 类型 - 字符串
- 说明 -（可选）要导入的 AnyConnect 配置文件（XML 格式或 XML 的 Base64 编码）

vpn_connection_device_id

- 标题 - 设备标识符
- 类型 - 字符串
- 说明 -（可选）报告给前端的设备标识符。如果未设置，AnyConnect 将生成随机的永久设备标识符。

vpn_connection_report_hardware_id

- 标题 - 报告硬件标识符（MAC 地址和 IMEI）以进行 VPN 身份验证
- 类型 - bool
- 说明 -（可选）AnyConnect 是否应尝试向前端报告硬件标识符。默认情况下，AnyConnect 会尝试报告硬件标识符（如果可访问）。

vpn_setting_allowed_saved_credentials

- 标题 - 允许用户保存凭证
- 类型 - bool

- 默认值 - false
- 说明 -（可选）是否允许用户保存凭证（需要屏幕锁定）。默认情况下，不允许用户保存凭证。

vpn_configuration_list

- 标题 - VPN 连接列表
- 类型 - bundle_array
- 说明 -（可选）使用此项配置多个连接条目。每个条目都是 vpn_configuration 捆绑包。

umbrella_org_id

- 标题 - Umbrella 组织 ID
- 类型 - 字符串
- 说明 - 客户所属的组织 ID，显示在从思科 Umbrella 控制板下载的配置文件中。

umbrella_reg_token

- 标题 - Umbrella 注册令牌
- 类型 - 字符串
- 说明 - 向组织颁发的唯一 regToken，值显示在从思科 Umbrella 控制板下载的配置文件中。

umbrella_va_fqdns

- 标题 - Umbrella VA FQDN 列表
- 类型 - 字符串
- 说明 - 这是连接的网络中存在的 VA 的 FQDN 列表。

admin_email

- 标题 - 管理员电子邮箱地址
- 类型 - 字符串
- 说明 -（可选）设置发送日志的默认管理员电子邮件地址。

vpn_always_on_umbrella_only

- 标题 - 仅对 Umbrella 保护启用永远在线 VPN 模式
- 类型 - bool
- 默认值 - false
- 说明 -（仅适用于使用 Umbrella 的情况下）如果设置为 true，则永远在线 VPN 将仅应用 Umbrella 保护。如果设置为 false，则永远在线 VPN 将应用于 Umbrella 和远程访问。

vpn_configuration 捆绑包的受管限制

vpn_name

- 标题 - 显示名称
- 类型 - 字符串
- 说明 - 用户友好名称（仅用于显示）。如果未设置，则默认为 host。

vpn_host

- 标题 - 主机
- 类型 - 字符串
- 说明 - 指向前端的 URL。此栏必填。

vpn_protocol

- 标题 - 协议
- 类型 - 选项
- 可能值 - SSL | IPsec
- 说明 - VPN 隧道协议（SSL 或 IPsec）。默认为 SSL。

vpn_ipsec_auth_mode

- 标题 - IPsec 身份验证模式
- 类型 - 选项
- 可能值 - EAP-AnyConnect | EAP-GTC | EAP-MD5 | EAP-MSCHAPv2 | IKE RSA
- 说明 -（可选）当隧道协议为 IPsec 时使用的身份验证模式。默认为 EAP-Connect。

vpn_ipsec_ike_identity

- 标题 - IKE 身份
- 类型 - 字符串
- 说明 -（可选）仅当 IPsec 身份验证模式为 EAP_GTC、EAP-MD5 或 EAP-MSCHAPv2 时适用。

vpn_keychain_cert_alias

- 标题 - 密钥链证书别名
- 类型 - 字符串
- 说明 -（可选）要用于此 VPN 配置的客户端证书的密钥链别名。

vpn_allowed_apps

- Key—vpn_allowed_apps

- 标题 - Per App VPN 允许的应用
- 类型 - 字符串
- 说明 -（可选）指定哪些应用（Android 应用软件包名称的逗号分隔列表）应建立隧道，从而启用 Per App VPN。所有其他应用都不建立隧道。此设置要求在前端上启用 Per-App VPN。

vpn_diallowed_apps

- 标题 - Per App VPN 禁止的应用
- 类型 - 字符串
- 说明 -（可选）指定哪些应用（Android 应用软件包名称的逗号分隔列表）不应建立隧道，从而启用 Per-App VPN。所有其他应用都建立隧道。此设置要求在前端上启用 Per-App VPN。

vpn_allow_bypass

- 标题 - 允许应用绕过 VPN 隧道
- 类型 - bool
- 说明 -（可选）允许应用绕过此 VPN 连接。默认情况下，此项为禁用状态。

vpn_set_active

- 标题 - 设置为活动状态：
- 类型 - bool
- 默认值 - false
- 说明 -（可选）将此设置为最后一个选择的 VPN 配置（如果没有任何配置）。

Apple iOS 设备上的 AnyConnect

有关此版本支持的功能和设备，请参阅适用于 Apple iOS 的 Cisco AnyConnect Secure Mobility Client 4.x 版发行说明。

Apple iOS 版 AnyConnect 准则和限制

Apple iOS 版 AnyConnect 仅支持与远程 VPN 接入相关的功能，例如：

- AnyConnect 可由用户手动配置、通过 iPhone 配置实用程序 (http://www.apple.com/support/iphone/enterprise/) 生成的 AnyConnect VPN 客户端配置文件配置或使用企业移动设备管理器配置。
- Apple iOS 设备仅支持一个 AnyConnect VPN 客户端配置文件。生成的配置内容始终与最近的配置文件匹配。例如，如果您连接到 vpn.example1.com，然后连接到 vpn.example2.com，则从 vpn.example2.com 导入的 AnyConnect VPN 客户端配置文件将替换从 vpn.example1.com 导入的配置文件。

- 此版本支持隧道保持连接功能；但是，它会降低设备电池的寿命。增加更新间隔值可以缓解此问题。

Apple iOS 按需连接注意事项：

- 当设备休眠时，由于 iOS 按需逻辑而自动连接的 VPN 会话及已配置“暂停时断开连接”的 VPN 会话会断开连接。唤醒设备后，按需逻辑将根据需要重新连接 CPN 会话。
- 启动用户界面和 VPN 连接后，AnyConnect 会收集设备信息。因此，如果用户在一开始或在设备信息（例如操作系统版本）变更后，依赖于 iOS 的按需连接功能来启动连接，AnyConnect 有时候可能误报移动安全评估信息。
- 使用 Apple 按需连接功能时，只有运行早于 4.0.05032 的旧版 AnyConnect 版本或早于 9.3 的 Apple iOS 版本，此功能才适用于您的环境。在更新 AnyConnect 后，为了确保正确建立按需连接 VPN 隧道，用户必须手动启动 AnyConnect 应用并建立连接。如果不这样做，在下次 iOS 系统尝试建立 VPN 隧道时，系统会显示错误消息“VPN 连接需要启动应用”(The VPN Connection requires an application to start up)。

思科 AnyConnect 和旧版 AnyConnect 是不同的应用，其应用 ID 有所不同。因此：

- 在 AnyConnect 4.0.07x（及更高版本）中使用新扩展框架会导致来自传统 AnyConnect 4.0.05x 的行为发生以下更改：AnyConnect 认为隧道 DNS 服务器的流量是通过隧道传输的，即使它不在拆分 - 包含网络中。
- 不能将 AnyConnect 应用从旧版 4.0.05x 或更早版本升级到 AnyConnect 4.0.07x 或 4.6.x（或更高版本）。Cisco AnyConnect 4.0.07x（或 4.6.x 和更高版本）是单独的应用，使用不同的名称和图标进行安装。
- AnyConnect 的不同版本可以共存于移动设备之上，但思科不支持此操作。如果在安装了两个 AnyConnect 版本时尝试进行连接，行为可能与预期不同。请确保您的设备上只有一个 AnyConnect 应用，并且其版本适合您的设备和环境。
- 新 AnyConnect 应用版本 4.0.07072 或更高版本不能访问或使用以旧版 AnyConnect 版本 4.0.05069 及任何更早版本导入的证书。两个应用版本均可访问和使用 MDM 部署的证书。
- 如果要更新至新版本，应删除导入到旧版 AnyConnect 应用的应用数据，例如证书和配置文件。否则，它们将继续显示在系统 VPN 设置中。在卸载旧版 AnyConnect 应用之前删除应用数据。
- 当前的 MDM 配置文件不会触发新应用。EMM 供应商必须支持 VPNType (VPN)、VPNSubType (com.cisco.anyconnect) 和 ProviderType (packet-tunnel)。为了与 ISE 集成，它们必须能够将唯一标识符传递给 AnyConnect，因为 AnyConnect 在新框架中不能再访问此信息。有关如何设置此功能，请咨询您的 EMM 供应商，有些可能需要自定义 VPN 类型，另一些在发布时可能无可用的支持。

在 AnyConnect 4.0.07x 及更高版本中使用新扩展框架会导致旧版 AnyConnect 4.0.05x 中的行为发生以下变化：

- 在新版本中，发送到前端的设备 ID 不再是 UDID，而且重置为出厂设置后，设备 ID 将发生变化，除非您的设备从其进行的备份中执行恢复。

- 您可以使用 MDM 部署的证书和使用 AnyConnect 中可用的某种方法导入的证书：SCEP、通过 UI 手动导入或通过 URI 处理程序导入。新版 AnyConnect 不能再使用通过邮件或识别的这些方法之外的任何其他机制导入的证书。
- 在使用 UI 创建连接条目时，用户必须接受显示的 iOS 安全消息。
- 用户创建的条目若与从 AnyConnect VPN 配置文件中下载的主机条目名称相同，当它们处于活动状态时，在断开连接前不会对其重命名。另外，断开连接后，下载的主机连接条目将出现在 UI 中，保持连接时则不会显示在 UI 中。
- AnyConnect 认为隧道 DNS 服务器的流量将通过隧道传输，即使它不在拆分 - 包含网络中。

Apple iOS 的特别注意事项

在 Apple iOS 设备上支持 AnyConnect 时，请注意：

- 本文档中的 SCEP 参考信息仅适用于 AnyConnect SCEP，不适用于 Apple iOS SCEP。
- 由于 Apple iOS 限制，通过 VPN 推送邮件通知不起作用。但是，当隧道策略从会话中排除外部可访问的 ActiveSync 连接时，AnyConnect 可以与这些连接并行工作。

Apple iPhone 配置实用程序

Windows 或 macOS 版本的 iPhone 配置实用程序 (IPCU) 用于对 Apple iOS 设备执行配置创建和部署过程，此程序可从 Apple 公司获取。此操作可代替在安全网关上配置 AnyConnect 客户端配置文件。

受 Apple 控制的现有 IPCU GUI 不了解 AnyConnect Ipsec 功能。在 IPCU 的现有 AnyConnect GUI 内配置 IPsec VPN 连接。按照“服务器”字段中的 RFC 2996 定义，使用以下 URI 语法。此“服务器”字段语法向后兼容记录的配置 SSL VPN 连接的用法。

[**ipsec**://][<**AUTHENTICATION**> [":" <**IKE-IDENTITY**> "@"]] <**HOST**> [":" <**PORT**>] ["/" <**GROUP-URL**>]

参数	说明
ipsec	：表示这是 IPsec 连接。如果省略，则假设是 SSL。
AUTHENTICATION	指定 IPsec 连接的身份验证方法。如果省略，则假设是 EAP-AnyConnect。有效值为： • EAP-AnyConnect • EAP-GTC • EAP-MD5 • EAP-MSCHAPv2 • IKE-RSA

参数	说明
IKE-IDENTITY	当 AUTHENTICATION 设置为 EAP-GTC、EAP-MD5 或 EAP-MSCHAPv2 时，指定 IKE 标识。用于其他身份验证设置时，此参数无效。
HOST	指定服务器地址。要使用的主机名或 IP 地址。
PORT	当前忽略，包括用于与 HTTP URI 方案保持一致。
GROUP=URL	附加到服务器名称的隧道组名称。

示例：

```
ipsec://EAP-AnyConnect@asa-gateway.example.com
ipsec://asa-gateway.example.com
```

要仅连接到符合标准的 Cisco IOS 路由器，请使用以下资源：

```
ipsec://eap-md5:<identity>@ios-gateway.example.com
```

按需连接的使用准则

Apple iOS 按需连接功能允许 Safari 等其他应用启动 VPN 连接。Apple iOS 根据为设备的活动连接条目配置的规则评估应用所请求的域。仅在符合以下所有条件时，Apple iOS 才代表应用建立 VPN 连接：

- VPN 连接尚未建立。
- 与 Apple iOS 按需连接兼容的应用请求域。
- 连接条目被配置为使用有效证书。
- 已在连接条目中启用 Connect On Demand。
- Apple iOS 无法将 Never Connect 列表中的字符串与域请求匹配。
- 满足以下任一条件：Apple iOS 匹配域请求“始终连接”列表中的字符串（仅限 Apple iOS 6）。或 DNS 查询失败，并且 Apple iOS 匹配域请求“按需连接”列表中的字符串。

使用按需连接功能时，请记住以下事项：

- 使用 iOS 的按需连接功能启动 VPN 连接后，如果隧道在特定时间间隔内处于不活动状态，iOS 将断开隧道连接。有关详细信息，请参阅 Apple 的 VPN 按需连接文档。
- 如果您配置规则，我们建议使用“需要时连接”(Connect if Needed) 选项。如果 DNS 查询内部主机失败，按需连接规则将启动 VPN 连接。它需要正确的 DNS 配置，以便企业中的主机名仅使用内部 DNS 服务器进行解析。
- 对于已配置按需连接的移动设备，基于证书的身份验证隧道组设有短暂（60 秒）的空闲超时 (vpn-idle-timeout)。如果您的 VPN 会话对于应用不是至关重要且无需始终保持连接，请设置短暂的空闲超时。苹果设备在不再需要 VPN 连接时（例如，设备进入休眠型号）会将其关闭。隧道组的默认空闲超时时间为 60 分钟。

- 始终连接的行为与版本有关：
  - 在 Apple iOS 6 上，iOS 在匹配此列表中的规则时始终会启动 VPN 连接。
  - 在 iOS 7.x 上，不支持“始终连接”。当此列表中的规则匹配时，其行为与 Connect If Needed 规则相同。
  - 在以后的版本中，不使用“始终连接”。配置的规则将跳转到 Connect if Needed 列表，并按照该规则操作。
- Apple 已针对按需连接功能推出了受信任的网络检测 (TND) 增强功能。此增强功能：
  - 通过确定设备用户是否位于受信任的网络中，扩展按需连接功能。
  - 仅适用于 Wi-Fi 连接。当通过其他类型的网络连接运行时，按需连接不使用 TND 来确定是否连接 VPN。
  - 不是独立功能，不能在按需连接功能之外配置或使用。

  请联系苹果公司，了解有关 iOS 6 中 Connect On Demand 值得信赖的网络检测的详细信息。
- 集成的 Apple iOS Ipsec 客户端和 AnyConnect 均使用相同的 Apple iOS VPN 按需连接框架。

利用分割隧道拆分 DNS 解析行为

ASA 分割隧道功能允许您指定哪种流量通过 VPN 隧道，哪种流量畅通无阻。一个称为拆分 DNS 的相关功能允许您指定哪种 DNS 流量适合通过 VPN 隧道进行 DNS 解析，哪种 DNS 流量由终端 DNS 解析器处理（畅通无阻）。拆分 DNS 在 Apple iOS 设备上与在其他设备（如果也配置了分割隧道）上的工作方式不同。Apple iOS 版本的 AnyConnect 对此命令的响应如下：

- 仅加密 split-dns 列表中所列域的 DNS 查询。

  AnyConnect 隧道仅允许对命令中指定域的 DNS 查询通过隧道。它会将所有其他 DNS 查询发送到本地 DNS 解析程序，以明文形式进行解析。例如，响应以下命令时，AnyConnect 仅通过隧道传输对 example1.com 和 example2.com 的 DNS 查询：

  ```
  hostname(config-group-policy)# split-dns value example1.com example2.com
  ```

- 仅加密 default-domain 命令中域的 DNS 查询。

  如果 **split-dns none** 命令存在，且 **default-domain** 命令指定了一个域，则 AnyConnect 仅通过隧道传输该域的 DNS 查询，而将所有其他 DNS 查询畅通无阻地发送到本地 DNS 解析器进行解析。例如，响应以下命令时，AnyConnect 仅通过隧道传输 example1.com 的 DNS 查询：

  ```
  hostname(config-group-policy)# split-dns none
  hostname(config-group-policy)# default-domain value example1.com
  ```

- 畅通无阻地发送所有 DNS 查询。如果 **split-dns none** 和 **default-domain none** 命令存在于组策略中，或者虽然这些命令不存在于组策略中，但存在于默认组策略中，则 AnyConnect 将所有 DNS 查询畅通无阻地发送到本地 DNS 解析器进行解析。

注释 如果未指定 split-dns，则组策略继承存在于默认组策略中的分割隧道域列表。要防止继承分割隧道域列表，请使用 split-dns none 命令。

适用于 iOS 的 YubiKey 证书验证

您可以使用 YubiKey 作为 VPN 证书身份验证的外部证书。要启用 Yubikey 功能，请将以下内容添加到 MDM VPN 配置文件的 VendorConfig 中：

YubiKeyCertSlot，有效时隙值为 9a、9c、9d 或 9e。

Yubikey 与其他智能卡/令牌设备不同，并且也同样不受支持。例如，在 ASA 默认组策略中配置的 **SmartCard 断开连接**命令对使用移动设备的 Yubikey 没有影响。

iOS 版 AnyConnect 的 MDM 可配置设置

定义 AnyConnect 本地安全设置

要在受管 Apple iOS 设备上定义 AnyConnect 本地安全设置，请使用 MDM 和以下密钥/值对更改默认值。当这些密钥或值对由 MDM 配置时，它们会推送到最终用户的设备。这些值（通过 MDM 配置设置）会禁止 AnyConnect 最终用户更改 AnyConnect UI 中的这些设置。

密钥	值	类型
UriExternalControl	Disabled/Prompt/Enabled	字符串
BlockUntrustedServers	true/false	布尔值
EnableFipsMode	true/false	布尔值
CheckCert Revocation	true/false	布尔值
StrictCertTrust	true/false	布尔值

阻止最终用户添加 VPN 连接

要阻止 AnyConnect 最终用户在受管 Apple iOS 设备上添加 VPN 连接，请使用 MDM 并将 BlockUserCreateVPNConnection 密钥设置为 *true* 值。通过 MDM 配置设置的这些值可防止 AnyConnect 最终用户添加 VPN 连接或导入配置文件。此外，将禁用 URI 处理以创建 VPN 连接或导入配置文件。如果未使用 MDM 设置此密钥或值对，最终用户将能够添加 VPN 连接（默认设置）。

Chrome OS 设备版 AnyConnect

有关此版本支持的功能和设备，请参阅适用于 Google Chrome 操作系统的 Cisco AnyConnect Secure Mobility Client 4.x 版发行说明。

在 Chrome 操作系统上使用 AnyConnect 的准则和限制

- 我们并未计划任何未来的 Chrome 操作系统版本。由于所有当前 ChromeBook 都支持 Android 应用，因此我们建议您改用 AnyConnect Android 应用。
- 当托管 Chromebook 设备（注册参加企业 Chrome 管理服务）时，AnyConnect 无法访问客户端证书：客户端证书身份验证不运行。
- 在低端 Chromebooks 上 VPN 性能受限（chromium 问题 #514341）。
- 51 或更高版本 Chrome 操作系统的 4.0.10113 或更高版 AnyConnect 支持自动重新连接（当网络接口断断续续时会重新连接 VPN 会话）。Chrome 51 及此 AC 版本发行之前，您如果丢失 Wi-Fi 连接或使设备休眠，AnyConnect 会无法自行重新连接。
- 除非使用 Chrome 操作系统 45 或更高版本，否则从安全网关收到的所有服务器证书，即使是完全受信任和有效的证书，也会被视为不可信。
- 在 Chrome 操作系统上安装或升级 AnyConnect 后，等到初始化完成后再配置 AnyConnect。AnyConnect 应用中会显示“正在初始化，请稍候…”（Initializing, please wait...）。这个过程会需要几分钟的时间。

通用 Windows 平台上的 AnyConnect

有关此版本支持的功能和设备，请参阅适用于通用 Windows 平台的 Cisco AnyConnect Secure Mobility Client 4.9.x 版发行说明。

通用 Windows 平台上的 AnyConnect 准则和限制

- 由于不支持 DTLS 和 IPsec/IKEv2 而导致性能受限。
- 不支持 VPN 漫游（在 WiFi 网络与 3/4G 网络之间转换）。
- 由用户断开的连接不会从前端完全断开。思科建议连接到提供短暂空闲超时的 ASA VPN 组，以便清除 ASA 上的孤立会话。
- 当移动设备用户连接到没有有效移动版许可证的 ASA 时，该用户将进入登录循环，即，输入凭证后，身份验证将重启，最后（经过 5 次尝试后）向用户发送一条通用错误消息：`VPN 连接失败，错误代码为 602 (The VPN connection has failed with error code 602)。请与您的管理员联系，确保在安全网关上安装有效的移动版许可证`

在 ASA 安全网关上配置移动设备 VPN 连接

步骤 1 请参阅相应版本的 思科 ASA 5500-X 系列下一代防火墙配置指南，以了解桌面和移动终端的通用配置过程。对于移动设备，请注意以下方面：

属性	ASDM 位置	例外
主页 URL	**Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add / Edit > Advanced > AnyConnect Client > Customization**	AnyConnect 移动将忽略主页 URL 设置。身份验证成功后，您无法重定向移动客户端。
AnyConnect 连接配置文件的名称和别名	**Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add / Edit**	请勿在用于 AnyConnect 移动客户端连接的隧道组（连接配置文件）的 Name 或 Aliases 字段中使用特殊字符。使用特殊字符可能导致 AnyConnect 客户端显示错误消息：`Connect attempt has failed` after logging that it is `Unable to process response from Gateway`。
Dead Peer Detection	配置 > 远程访问 VPN > 网络（客户端）访问 > 组策略 > 添加/编辑 > 高级 > AnyConnect 客户端	关闭服务器端的失效对等检测，因为它会阻止设备休眠。但是，客户端的失效对等项检测应保持开启，因为它使客户端可以确定隧道何时由于缺少网络连接而终止。
SSL 保持连接消息 (SSL Keepalive Messages)	**Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add / Edit > Advanced > AnyConnect Client**	我们建议禁用这些保持连接消息，以保护移动设备的电池寿命，尤其是在启用客户端失效对等项检测的情况下。
IPsec over NAT-T 保持连接消息 (IPsec over NAT-T Keepalive Messages)	配置 > 远程访问 VPN > 网络（客户端）访问 > 高级 > IPsec > IKE 参数	必须选择**启用 IPsec over NAT-T (Enable IPsec over NAT-T)** 以使 AnyConnect IPsec 工作。启用时，默认情况下每 20 秒发送 NAT 保持连接消息，导致移动设备用电过度。 为了最大限度地降低对移动设备设备电量消耗的影响，我们建议您将 NAT-T Keepalive 设为最大值 3600，因为这些消息无法禁用。 使用 `crypto isakmp nat-traversal 3600` 命令在 ASA CLI 中指定此设置。

步骤 2 配置移动终端安全评估（也称为 AnyConnect 身份扩展，ACIDex），以根据需要接受、拒绝或限制移动连接。

请参阅思科 ASA 5500-X 系列下一代防火墙配置指南相应版本中的配置 *DAP* 中使用的终端属性程序。

示例：

当建立连接时，以下属性由 Apple iOS 上的 AnyConnect 发送到前端：

```
endpoint.anyconnect.clientversion="4.0.03004";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.devicetype="iPhone7,2";
endpoint.anyconnect.platformversion="9.0";
endpoint.anyconnect.deviceuniqueid="11025f84e99351e807f3583343bfec96351cb416";
```

步骤 3 （可选） 配置 Per App VPN 隧道型号。

请参阅配置 Per App VPN， 第 267 页。

如果未配置 Per App VPN 隧道型号，则 AnyConnect 应用在系统隧道型号下运行。

配置 Per App VPN

开始之前

AnyConnect Per App VPN 隧道需要：

- ASA 9.3.1 或更高版本以配置 Per App VPN 隧道。
- AnyConnect v4.0 Plus 或 Apex 许可证。

AnyConnect Per App VPN 支持以下移动平台：

- 运行 Android 5.0 (Lollipop) 或更高版本的 Android 设备。
- 运行 Apple iOS 8.3 或更高版本的 Apple iOS 设备，配置为在移动设备管理 (MDM) 解决方案中使用 Per App VPN。

步骤 1 安装 Cisco AnyConnect 企业应用选择器工具， 第 268 页。

步骤 2 确定隧道中允许的应用， 第 268 页。

步骤 3 确定哪些应用程序应该绕过隧道， 第 269 页。

步骤 4 确定移动应用的应用 ID， 第 269 页。

步骤 5 配置 Per App VPN， 第 267 页。

步骤 6 使用应用程序选择器工具为您的平台指定 AnyConnect Per App VPN 策略：

- 为 Android 设备定义 Per-App VPN 策略， 第 270 页
- 为 Apple iOS 设备定义 Per App VPN 策略， 第 271 页

步骤 7 创建 Per App 定制属性， 第 271 页（在 ASA 上）。

步骤 8 将定制属性分配到 ASA 上的策略， 第 272 页。

安装 Cisco AnyConnect 企业应用选择器工具

应用选择器工具是一个独立应用，支持为 Android 和 Apple iOS 设备生成策略。

开始之前

Cisco AnyConnect 企业应用选择器需要 Java 7 或更高版本。

步骤 1 从 Cisco.com AnyConnect 安全移动客户端 v4.x 软件中心 下载 Cisco AnyConnect 企业应用选择器工具。

步骤 2 如果您在策略中使用的是 Android 应用，则必须在系统中安装 Android SDK 和 Android SDK 构建工具。否则，请按如下方式安装它们。

a) 为您运行应用选择器工具所在的平台安装最新版本的 Android SDK 工具。

使用默认路径和设置为您的平台安装建议的**仅 SDK 工具**软件包，包括：安装 All Users（所有用户），以便按照所述访问软件包实体。

b) 使用 Android SDK 管理器，安装最新版本的 **Android SDK Build-tools**。

下一步做什么

注释 如果在应用选择器工具中收到提示，请配置对 Android 资产打包工具 **aapt** 的访问，方法是指定其安装位置 *Android SDK installation directory*\build-tools*build-tools version number*\。

确定隧道中允许的应用

当您支持移动设备（例如运行 Android 或 iOS 的手机）时，您可以使用移动设备管理器 (MDM) 应用微调 VPN 访问，以仅允许支持的应用使用 VPN 隧道。通过将远程访问 VPN 限制为批准的应用，您可以减少 VPN 前端的负载，也可以保护企业网络免受这些移动设备上安装的恶意应用的影响。

要使用基于每个应用的远程访问 VPN，您必须安装和配置第三方 MDM 应用。在 MDM 中，您要定义可通过 VPN 隧道使用的已批准应用的列表。说明如何配置和使用所选的第三方 MDM 不在本文档的讨论范围内。

当您使用 AnyConnect 从移动设备建立 VPN 连接时，所有流量（包括来自个人应用的流量）都通过 VPN 路由。如果您想只通过 VPN 路由公司应用，以便从 VPN 中排除非公司流量，可以使用 Per-App VPN 选择哪些应用通过 VPN 进行隧道连接。

配置 Per-App VPN 具有以下主要优点：

- 性能 - 它将 VPN 中的流量限制为需要进入企业网络的流量。因此，您可以释放 RA VPN 前端的资源。

- 保护 - 由于只允许来自批准的应用的流量，因此可保护公司隧道免受用户可能无意间在移动设备上安装的未批准恶意应用的影响。由于这些应用不包括在隧道中，因此来自这些应用的流量永远不会发送到前端。

移动终端上运行的移动设备管理器 (MDM) 在应用上强制实施 Per-App VPN 策略。

确定哪些应用程序应该绕过隧道

您可以使用移动设备管理器 (MDM) 应用来确定 VPN 访问，并指定要绕过隧道并在公共接口转出的任何应用。此选项允许的功能类似于桌面上 AnyConnect 提供的动态分割隧道功能。

您必须安装和配置第三方 MDM 应用。在 MDM 中，您可以定义要绕过 VPN 隧道的应用程序列表。本文档未对如何配置和使用第三方 MDM 进行介绍，但在移动终端上运行的 MDM 会根据 Per-App VPN 策略来强制实施哪些应用程序排除项。在 MDM 中，设置 Android 配置框架密钥值对，同时定义要支持哪些密钥。通过 MDM Android 托管配置，就像为要通过隧道的任何应用程序选择 **vpn_connection_allowed_apps** 一样，您也可以为要绕过隧道的任何应用程序选择 **vpn_connection_disallowed_apps**。然后，提供要排除或包含的应用程序 ID 列表，以逗号分隔。

两个设置均要求在前端上启用 Per-App VPN。例如：

- `string name="restriction_perapp_include_desc"`

  指定应通过隧道传输的应用程序，从而启用 per-app VPN。所有其他应用程序都不会建立隧道。

- `string name="restriction_perapp_include_desc"`

  指定哪些应用程序应绕过隧道，从而启用 per-app VPN。这些应用程序可用于公共接口，而所有其他应用程序都通过隧道传输。

确定移动应用的应用 ID

我们强烈建议您在选择在用户移动设备上提供服务的移动设备管理器 (MDM) 中配置 Per-App 策略。这样可以极大简化前端配置。

如果您决定还要在前端或阻止的应用程序列表上配置允许的应用列表，则需要确定每种类型的终端上每个应用的应用 ID。

应用 ID（在 iOS 中称为捆绑包 ID）是反向 DNS 名称。您可以使用星号作为通配符。例如，*.* 表示所有应用，com.cisco.* 表示所有 Cisco 应用。

- Android - 在网络浏览器中转至 Google Play，然后选择应用类别。单击要允许（或不允许）的应用（或将鼠标悬停在该应用上），然后查看 URL。应用 ID 位于 URL 中的 **id=** 参数上。例如，Facebook Messenger 的 URL 如下，因此应用 ID 是 com.facebook.orca：

  `https://play.google.com/store/apps/details?id=com.facebook.orca`

对于通过 Google Play 无法获得的应用（例如您自己的应用），下载一个程序包名称查看器应用以提取该应用 ID。Cisco 不为任何可用的应用背书，但这些应用之一应能够满足您的需求。

- iOS - 查找捆绑包 ID 的方式之一：

1. 使用桌面浏览器（例如 Chrome）搜索应用名称。
2. 在搜索结果中，查找从 Apple App Store 下载该应用的链接。例如，Facebook Messanger 的下载链接类似于 https://apps.apple.com/us/app/messenger/id454638411。
3. 复制 **id** 字符串后面的数字。在本例中，即 **454638411**。
4. 打开一个新的浏览器窗口，然后将该数字添加到以下 URL 的末尾：

   `https://itunes.apple.com/lookup?id=`

   在本例中，即为 https://itunes.apple.com/lookup?id=454638411
5. 系统将提示您下载文本文件，该文件通常命名为 1.txt。下载文件。
6. 在文本编辑器（例如写字板）中打开文件，然后搜索 bundleId。例如："bundleId":"com.facebook.Messenger"。在本例中，捆绑包 ID 为 com.facebook.Messenger。以此作为应用 ID。

拥有应用 ID 列表后，您可以配置策略。

为 Android 设备定义 Per-App VPN 策略

Per-app VPN 策略包含一组规则，其中每条规则标识数据在隧道中流动的应用。指定规则选项以在移动设备环境中更严格地标识允许的应用及其使用。您需要在 ASA 上配置某种 Per-app 策略（自定义属性），以便 Per-app 正常运行，即使已为 Per-app 配置了 MDM。“应用程序选择器”(Application Selector) 工具使用来自应用的软件包文件 `*.apk` 的信息可设置规则选项。有关 Android 软件包的清单信息，请参阅 http://developer.android.com/guide/topics/manifest/manifest-element.html。

开始之前

Cisco AnyConnect 企业应用选择器需要 Java 7 或更高版本。

步骤 1 启动应用选择器，并选择 **Android** 移动设备平台。

步骤 2 设置所需的**应用 ID (App ID)** 字段。

- 选择**从磁盘导入 (Import from Disk)**，以便从本地系统存储的应用中获取特定于应用的软件包信息。

  “APP ID”字段（反式 DNS 格式的字符串）会自动填入。例如，如果选择适用于 Apple iOS 策略的 Chrome 应用，“APP ID”字段将设置为 **`com.google.chrome.ios`**。对于 Android 上的 Chrome，它将设置为 **`com.android.chrome`**。
- 或者，您也可以直接输入此特定于应用的信息。
- 使用通配符指定反向 DNS 格式，例如，指定 com.cisco.* 以通过隧道传送所有思科应用，而不是在各自的规则中列出每个应用。通配符必须是“应用 ID”(APP ID) 条目中的最后一个字符。

  在托管环境中配置 Per-app VPN 时，请确保 ASA 策略与 MDM 策略允许相同的应用通过隧道。我们建议指定 *.* 为应用 ID，以允许所有应用通过隧道，并确保 MDM 策略是隧道应用的唯一仲裁者。非 *.* 策略不受支持。

步骤 3 （可选） 选择列出的应用，并根据需要配置更多参数。

- 最低版本 - 软件包清单属性 *android: versionCode* 中指定的所选应用的最低版本。
- 匹配证书 ID - 签署证书的应用摘要。
- Allow Shared UID - 默认值为 true。如果设置为 false，具有软件包清单中指定的 *android: sharedUserId* 属性的应用将不匹配此规则，并会被阻止访问隧道。

步骤 4 单击**文件 (File) > 保存 (Save)**以保存此 Per-app VPN 策略。

步骤 5 选择**策略 (Policy) > 查看策略 (View Policy)** 查看已定义策略的表示。

复制此字符串。此字符串将成为 ASA 上自定义属性 *perapp* 的值。

为 Apple iOS 设备定义 Per App VPN 策略

Apple iOS 设备上的 Per App VPN 策略完全由 MDM 设施控制。因此，AnyConnect 必须允许所有应用，而 MDM 必须配置 per app 策略来指定可通过隧道的特定应用。

开始之前

Cisco AnyConnect 企业应用选择器需要 Java 7 或更高版本。

步骤 1 启动应用选择器，并选择 **Apple iOS** 移动设备平台。

步骤 2 将所需的 **App ID** 字段设置为 ***.***。

此设置允许所有应用通过 AnyConnect 隧道，并可确保 MDM per app 策略是隧道应用的唯一仲裁者。

步骤 3 单击**文件 (File) > 保存 (Save)** 以保存此 Per App VPN 策略。

步骤 4 选择**策略 (Policy) > 查看策略 (View Policy)** 查看已定义策略的表示。

复制此字符串。此字符串将成为 ASA 上自定义属性 *perapp* 的值。

创建 Per App 定制属性

步骤 1 在 ASDM 中，导航到 **Configuration > Remote Access VPN > Network (Client) Access> Advanced > AnyConnect Custom Attributes** 以配置定制属性类型。

步骤 2 选择**添加 (Add)** 或**编辑 (Edit)** 并在**创建/编辑自定义属性类型 (Create / Edit Custom Attribute Type)** 窗格中设置以下项：

a) 将 *perapp* 输入为类型。

类型必须是 *perapp*，因为这是 AnyConnect 客户端唯一可识别的 Per App VPN 属性类型。将此属性添加到远程访问 VPN 组配置文件会自动将隧道限制到明确标识的平台。来自所有其他应用的流量将自动从隧道中排除。

b) 输入您选择的描述。

步骤 3 单击**确定 (OK)** 关闭此窗格。

步骤 4 导航到 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names** 以配置定制属性。

步骤 5 选择**添加 (Add)** 或**编辑 (Edit)** 并在**创建/编辑自定义属性名称 (Create / Edit Custom Attribute Name)** 窗格中设置以下项：

a) 选择 *perapp* 属性 **Type**。

b) 输入 **Name**。此名称用于向策略分配此属性。

c) 选择**添加 (Add)**，可通过从策略工具复制 BASE64 格式并将其粘贴在此处来一个或多个值。

每个值不得超过 420 个字符。如果值超过此长度，请为其他值内容添加多个值。配置的值在发送到 AnyConnect 客户端之前会合并。

将定制属性分配到 ASA 上的策略

perapp 定制属性可以分配到组策略或动态访问策略。

步骤 1 打开 ASA 上的策略：

- 对于组策略，导航到 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add / Edit > Advanced > AnyConnect Client > Custom Attributes**。
- 对于动态访问策略，导航到 **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies Add / Edit**。在**访问/授权策略属性 (Access/Authorization Policy Attributes)** 部分中，选择 **AnyConnect 自定义属性 (AnyConnect Custom Attributes)** 选项卡。

步骤 2 单击**添加 (Add)** 或**编辑 (Edit)** 添加或编辑现有属性，从而打开**创建/编辑自定义属性 (Create / Edit Custom Attribute)** 窗格。

步骤 3 从下拉列表中选择预定义的 *perapp* 属性类型。

步骤 4 选择**选择值 (Select Value)**，然后从下拉列表中选择预定义的值。

步骤 5 单击**确定 (OK)** 关闭打开的配置窗格。

在 AnyConnect VPN 配置文件中配置移动设备连接

AnyConnect VPN 客户端配置文件是指定客户端行为并定义 VPN 连接条目的 XML 文件。每个连接条目指定一个可访问终端设备及其他连接属性、策略和条件的安全网关。使用 AnyConnect 配置文件编辑器来创建 VPN 客户端配置文件，其中包括移动设备的主机连接条目。

用户无法修改或删除从 ASA 传输到移动设备的 VPN 配置文件中定义的连接条目。用户只能修改和删除其手动创建的连接条目。

在任一时刻，AnyConnect 在移动设备上只保留一个当前 VPN 客户端配置文件。在启动自动或手动 VPN 连接后，新的 VPN 配置文件完全取代当前配置文件。如果用户手动删除当前配置文件，则会删除此配置文件，同时删除此配置文件中定义的所有连接条目。

步骤 1 配置基本 VPN 访问。

请参阅配置 VPN 访问，第 105 页，了解桌面和移动终端通用的处理以下例外的程序：

配置文件属性	例外
Auto Reconnect	对于 Apple iOS 之外的所有平台，无论自动连接如何规定，AnyConnect 移动版始终会尝试 ReconnectAfterResume。 仅 Apple iOS 支持暂停时断开连接 (Disconnect on Suspend)。当选择“暂停时断开连接”(Disconnect on Suspend) 时，AnyConnect 将断开连接并释放分配到 VPN 会话的资源。只有用户手动连接或配置了按需连接，它才会作出响应而重新连接。
本地局域网接入	AnyConnect 移动版将忽略本地 LAN 接入设置，始终允许本地 LAN 接入，无论客户端配置文件中的设置如何。

步骤 2 配置移动特定属性：

a) 在 VPN 客户端配置文件中，选择导航窗格中的**服务器列表 (Server List)**。
b) 选择**添加 (Add)** 将新服务器条目添加至列表，或从列表中选择服务器条目并按**编辑 (Edit)** 打开“服务器列表条目”(Server List Entry) 对话框。
c) 配置特定于移动设备的参数。
d) 单击**确定 (OK)**

步骤 3 使用以下方式之一来分发 VPN 客户端配置文件：

- 配置 ASA 以在建立 VPN 连接后将客户端配置文件上传到移动设备。

  请参阅AnyConnect 配置文件编辑器，第 73 页章节，了解关于如何将 VPN 客户端配置文件导入 ASA 并将其与组策略相关联的说明。

- 向用户提供 AnyConnect URI 链接以导入客户端配置文件。（仅限 Android 和 Apple iOS）

  请参阅导入 VPN 客户端配置文件，第 280 页，为您的用户提供这种部署过程。

- 让用户使用移动设备上的 **Profile Management** 来导入 AnyConnect 配置文件。（仅限 Android 和 Apple iOS）

  有关特定于设备的程序，请参阅相应的移动设备用户指南。

使用 URI 处理程序自动执行 AnyConnect 操作

AnyConnect 中的 URI 处理程序可让其他应用以通用资源标识符 (URI) 的形式向 AnyConnect 传递操作请求。为简化 AnyConnect 用户设置过程，请将 URI 嵌入网页或电邮消息上的链接，并且向用户提供访问说明。

开始之前

- AnyConnect 中的 URI 处理程序可让其他应用以通用资源标识符 (URI) 的形式向 AnyConnect 传递操作请求。

  在托管环境中：

  外部控制在启用后允许所有 URI 命令，而无需用户交互。设置提示后，用户会收到 URI 活动的通知，然后可在请求时选择允许或不允许该活动。如果您使用提示，则应该告知用户如何响应与 URI 处理相关的提示。用于在 MDM 上配置设置的密钥和值包括：

  密钥 - *UriExternalControl*

  值 - 已启用、提示或已禁用

  注释 在 MDM 中完成配置设置并向下推送到用户设备后，不允许用户对此设置进行更改。

  在非托管环境中：

  AnyConnect 应用中的 URI 处理默认禁用。移动设备用户通过将 **External Control** 应用设置设为 Enable 或 Prompt 来允许此功能。外部控制在启用后允许所有 URI 命令，而无需用户交互。设置提示后，用户会收到 URI 活动的通知，然后可在请求时选择允许或不允许该活动。

- 输入 URI 处理程序参数值时，必须使用 URL 编码。使用工具（例如此链接中的工具）对操作请求编码。此外，请参阅下面提供的示例。
- 在 URI 中，`%20` 代表空格、`%3A` 代表冒号 (:)、`%2F` 代表正斜线 (/)、`%40` 代表 @ 符号。
- URI 中的斜线是可选的。

向用户提供以下任何操作的说明。

生成 VPN 连接条目

使用此 AnyConnect URI 处理程序可简化用户生成 AnyConnect 连接条目。

anyconnect:[//]**create**[/]**?name**=*Description***&host**=*ServerAddress*[**&Parameter1**=*Value***&Parameter2**=*Value* ...]

准则

- *host* 参数是必需的。所有其他参数均可选择。在设备上执行操作时，AnyConnect 会保存您输入到与 *name* 和 *host* 相关联的连接条目的所有参数值。
- 对要添加到设备的每个连接条目使用单独的链接。不支持在单个链路中指定多个创建连接条目操作。

参数

- **name**- AnyConnect 主屏幕的连接列表和 AnyConnect 连接条目的 Description 字段中显示的连接条目的唯一名称。AnyConnect 仅在名称唯一时才响应。建议名称不超过 24 个字符，以确保能正常显示在连接列表中。在字段中输入文本时，使用设备上显示的键盘上的字母、数字或符号。字母区分大小写。
- **host**- 输入要连接的 ASA 的域名、IP 地址或组 URL。AnyConnect 会将此参数的值插入 AnyConnect 连接条目的“服务器地址”(Server Address) 字段中。

```
anyconnect://create/?name=SimpleExample&host=vpn.example.com
anyconnect:create?name=SimpleExample&host=vpn.example.com
```

- **protocol** protocol（可选，如果未指定，则默认为 SSL）- 用于此连接的 VPN 协议。有效值为：
  - SSL
  - IPSec

```
anyconnect:create?name=ExampleIPsec&host=vpn.company.com&protocol=IPsec
```

- **authentication** （可选，仅当协议指定为 IPsec 时适用，默认为 EAP-AnyConnect）- 用于 IPsec VPN 连接的身份验证方法。有效值为：
  - EAP-AnyConnect
  - EAP-GTC
  - EAP-MD5
  - EAP-MSCHAPv2
  - IKE-RSA
- **ike-identity** （身份验证设置为 EAP-GTC、EAP-MD5 或 EAP-MSCAPv2 时需要）- 在 AUTHENTICATION 设置为 EAP-GTC、EAP-MD5 或 EAP-MSCHAPv2 时的 IKE 身份。用于其他身份验证设置时，此参数无效。

```
anyconnect:create?name=Description&host=vpn.company.com&protocol=IPsec
&authentication=eap-md5&ike-identity=012A4F8B29A9BCD
```

- **netroam** （可选，仅适用于 Apple iOS）- 确定是否限制在设备唤醒后或连接类型（例如 EDGE、3G 或 Wi-Fi）更改后重新连接所需的时间。此参数不影响数据漫游或使用多个移动服务运营商。有效值为：

- true -（默认值）此选项可优化 VPN 访问。AnyConnect 在 AnyConnect 连接条目的 Network Roaming 字段中插入值 ON。如果 AnyConnect 失去连接，它将尝试建立新连接，直到成功为止。此设置让应用依赖于与 VPN 的持续连接。AnyConnect 不限制重新连接所需的时间。
- false - 此选项可延长电池寿命。AnyConnect 将此值与 AnyConnect 连接条目的 Network Roaming 字段中的 OFF 值关联。如果 AnyConnect 失去连接，它在 20 秒内会一直尝试建立新连接，之后停止尝试。如有必要，用户或应用必须启动新的 VPN 连接。

```
anyconnect:create?name=Example%201&host=vpn.example.com&netroam=true
```

- **keychainalias**（可选）- 从系统证书存储区导入证书到 AnyConnect 证书存储区。此选项仅适用于 Android 移动平台。

  如果指定的证书不在系统存储区，系统会首先提示用户选择并安装该证书，再提示用户允许或拒绝将其复制到 AnyConnect 存储区。在移动设备上必须启用外部控制。

  以下示例将创建一个名为 *SimpleExample* 的新连接条目，该条目的 IP 地址设置为 *vpn.example.com*，并分配有名为 *client* 的证书用于身份验证。

  ```
  anyconnect://create/?name=SimpleExample&host=vpn.example.com&keychainalias=client
  ```

- **usecert**（可选）- 确定在建立与主机的 VPN 连接时是否使用设备上安装的数字证书。有效值为：
  - true（默认设置）- 允许建立与主机的 VPN 连接时自动选择证书。将 usecert 改为 true 而不指定 certcommonname 值，会将“证书”(Certificates) 字段设为“自动”(Automatic)，导致在连接时从 AnyConnect 证书存储区中选择证书。
  - false - 禁用自动选择证书。

  ```
  anyconnect:create?name=Example%201&host=vpn.example.com&usecert=true
  ```

- **certcommonname**（可选，但需要 usecert 参数）- 与设备上预装的有效证书的公用名称匹配。AnyConnect 将该值插入 AnyConnect 连接条目的 Certificate 字段中。

  要查看设备上安装的此证书，请单击**诊断 (Diagnostics)** > **证书 (Certificates)**。您可能需要滚动才能看到主机需要的证书。单击详细信息披露按钮可查看从证书读取的“公共名称”(Common Name) 参数及其他值。

- **useondemand**（可选，仅适用于 Apple iOS，并且要求 usecert、certcommonname 参数和以下域规范）- 确定应用（如 Safari）是否可以启动 VPN 连接。有效值为：
  - false（默认值）- 阻止应用启动 VPN 连接。使用此选项是阻止发出 DNS 请求的应用潜在触发 VPN 连接的唯一方式。AnyConnect 将此选项与 AnyConnect 连接条目的“按需连接”(Connect on Demand) 字段中的 OFF 值相关联。
  - true - 允许应用使用 Apple iOS 启动 VPN 连接。如果将 useondemand 参数设置为 true，AnyConnect 将在 AnyConnect 连接条目的 Connect on Demand 字段中插入 ON 值。（如果 useondemand = true，则需要 domainlistalways 或 domainlistifneeded 参数）

  ```
  anyconnect:create?name=Example%20with%20certificate&host=vpn.example.com
  &netroam=true&usecert=true&certcommonname=example-ID&useondemand=true
  &domainlistalways=email.example.com,pay.examplecloud.com
  &domainlistnever=www.example.com&domainlistifneeded=intranet.example.com
  ```

- **domainlistnever**（可选，要求 useondemand = true）- 列出域以评估是否符合取消使用 Connect on Demand 功能的条件。此列表是 AnyConnect 用于评估域请求是否匹配的第一个列表。如果域请求匹配，AnyConnect 将忽略该域请求。AnyConnect 将此列表插入 AnyConnect 连接条目的 Never Connect 字段中。此列表可让您排除特定资源。例如，您可能不想通过面向公众的 Web 服务器自动进行 VPN 连接。示例值为 `www.example.com`。
- **domainlistalways**（如果 useondemand=true，则需要 domainlistalways 或 domainlistifneeded 参数）- 列出域以评估是否匹配 Connect on Demand 功能。此列表是 AnyConnect 用于评估域请求是否匹配的第二个列表。如果应用请求访问此参数指定的域之一，并且尚未进行 VPN 连接，则 Apple iOS 会尝试建立 VPN 连接。AnyConnect 会将此列表插入 AnyConnect 连接条目的 Always Connect 字段中。示例值列表是 `email.example.com,pay.examplecloud.com`。
- **domainlistifneeded**（如果 useondemand=true，则需要 domainlistalways 或 domainlistifneeded 参数）- 如果发生 DNS 错误，AnyConnect 将根据此列表评估域请求是否匹配。如果此列表中有字符串和域匹配，Apple iOS 会尝试建立 VPN 连接。AnyConnect 会将此列表插入 AnyConnect 连接条目的 Connect If Needed 字段中。此列表最常用于对通过企业局域网无法访问的内部资源获取短时间访问权限。示例值为 `intranet.example.com`。

使用以逗号分隔的列表指定多个域。按需连接规则仅支持域名，而不支持 IP 地址。但 AnyConnect 灵活支持每个列表条目的域名格式，如下所示：

匹配	说明	示例条目	示例匹配	示例匹配失败
仅限准确的前缀和域名。	输入前缀、点和域名。	email.example.com	email.example.com	www.example.com email.1example.com email.example1.com email.example.org
任何具有准确域名的前缀。前导点可阻止连接到以 * example.com（例如 notexample.com）结尾的主机。	输入一个点，后面紧跟要匹配的域名。	.example.org	anytext.example.org	anytext.example.com anytext.1example.org anytext.example1.org
以您指定的文本结尾的任何域名。	输入要匹配的域名的末尾部分。	example.net anytext.	anytext-example.net anytext.example.net	anytext.example1.net anytext.example.com

建立 VPN 连接

使用此 AnyConnect URI 处理程序可连接到 VPN，以便用户轻松建立 VPN 连接。您还可以在 URI 中嵌入附加信息以执行以下任务：

- 预填用户名和密码

- 预填用于双重身份验证的用户名和密码
- 预填用户名和密码，并指定连接配置文件别名

此操作需要 name 或 host 参数，但允许同时使用以下语法之一：

anyconnect:[//]**connect**[/]**?**[**name=***Description*|**host=***ServerAddress*]
[**&Parameter1**=*Value***&Parameter2**=*value* ...]

或

anyconnect:[//]**connect**[/]**?name=***Description***&host=***ServerAddress*
[**&Parameter1**=*value***&Parameter2**=*value* ...]

指南

- 如果语句中的所有参数值与设备上 AnyConnect 连接条目中的参数值都匹配，则 AnyConnect 将使用其余参数建立连接。
- 如果 AnyConnect 无法使语句中的所有参数与连接条目中的参数匹配，并且 name 参数是唯一的参数，则它会生成一个新连接条目，然后尝试 VPN 连接。
- 仅在使用一次性密码 (OTP) 基础设施时，才应该在使用 URI 建立 VPN 连接时指定密码。

参数

- **name**- 连接条目的名称与在 AnyConnect 主窗口的连接列表中显示的名称相同。AnyConnect 根据 AnyConnect 连接条目的 Description 字段评估此值，如果使用前述说明在设备上创建了连接条目，则也曾调用 name。此值区分大小写。
- **host**- 输入域名、IP 地址或 ASA 的组 URL 以匹配 AnyConnect 连接条目的 Server Address 字段，如果使用前述说明在设备上生成了连接条目，则也曾调用 host。

  在 ASDM 中配置组 URL 的方法是选择 **“配置”(Configuration) >“远程访问 VPN”(Remote Access VPN) >“网络 (客户端) 访问”(Network (Client) Access) >“AnyConnect 连接配置文件”(AnyConnect Connection Profiles) >“高级”(Advanced) >“组别名/组 URL”(Group Alias/Group URL) >“组 URL”(Group-URL)**。
- **onsuccess**- 在连接成功时执行此操作。平台特定的行为：
  - 对于 Apple iOS 设备，指定在此连接转换到已连接状态时要打开的 URL，或使用 anyconnect:close 命令关闭 AnyConnect GUI。
  - 对于 Android 设备，指定在此连接转换为已连接状态或已处于已连接状态时要打开的 URL。可指定多个 onsuccess 操作。AnyConnect 始终在 Android 设备上连接成功后关闭 GUI。
- **onerror**- 连接失败时执行此操作。平台特定的行为：
  - 对于 Apple iOS 设备，指定在此连接失败时要打开的 URL，或使用 anyconnect:close 命令关闭 AnyConnect GUI。
  - 对于 Android 设备，指定在此连接失败时要打开的 URL。可指定多个 onerror 操作。AnyConnect 始终在 Android 设备上连接失败后关闭 GUI。

- **prefill_username**- 提供连接 URI 中的用户名并将其预填到连接提示中。
- **prefill_password**- 提供连接 URI 中的密码并且将其预填到连接提示中。此字段应仅用于为一次性密码配置的连接配置文件。
- **prefill_secondary_username**- 在配置为需要双重身份验证的环境中，此参数提供连接 URI 中的辅助用户名，并且将其预填到连接提示中。
- **prefill_secondary_password**- 在配置为需要双重身份验证的环境中，此参数提供连接 URI 中辅助用户名的密码，并且将其预填到连接提示中。
- **prefill_group_list**— 选择 **配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络 (客户端) 访问 (Network (Client) Access) > AnyConnect 连接配置文件 (AnyConnect Connection Profiles) > 高级 (Advanced) > 组别名/组 URL (Group Alias/Group URL) > 连接别名 (Connection Aliases)** 可在 ASDM 中定义的连接别名。

示例

- 在组 URI 中提供连接名称和主机名或组 URL：

```
anyconnect://connect/?name=Example
```

```
anyconnect:connect?host=hr.example.com
```

```
anyconnect:connect?name=Example&host=hr.example.com
```

```
anyconnect://connect/?name=Example&host=hr.example.com/group-url
&prefill_username=user1&prefill_password=password1
```

- 提供针对成功或失败的操作

  使用 onsuccess 或 onerror 参数可根据连接操作的结果开始打开指定的 URL：

```
anyconnect://connect?host=vpn.company.com
&onsuccess=http%3A%2F%2Fwww.cisco.com
```

```
anyconnect://connect?host=vpn.company.com
&onerror=http%3A%2F%2Fwww.cisco.com%2Ffailure.html
&onsuccess=http%3A%2F%2Fwww.cisco.com
```

  在 Android 上可以指定多个 onsuccess 操作：

```
anyconnect://connect?host=vpn.company.com
&onerror=http%3A%2F%2Fwww.cisco.com%2Ffailure.html
&onsuccess=http%3A%2F%2Fwww.cisco.com
&onsuccess=tel:9781111111
```

  在 Apple iOS 设备上，anyconnect://close 命令可在 onsuccess 或 onerror 参数中用来关闭 AnyConnect GUI：

```
anyconnect://connect?host=vpn.company.com
&onsuccess=anyconnect%3A%2F%2Fclose
```

- 提供连接信息并在 URI 中预填用户名和密码：

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
```

```
anyconnect:connect?name=Example&host=hr.example.com/group-url
&prefill_username=user1&prefill_password=password1
```

- 为双重身份验证提供连接信息并预填用户名和密码：

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
&prefill_secondary_username=user2&prefill_secondary_password=password2
```

- 提供连接信息、预填用户名和密码，并指定连接配置文件别名：

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
&prefill_group_list=10.%20Single%20Authentication
```

断开 VPN 连接

使用此 AnyConnect URI 处理程序可将用户从 VPN 断开。

anyconnect:[//]**disconnect**[/]**&onsuccess=**URL

参数

onsuccess 参数仅适用于 Android 设备。指定 URL 在此连接断开或已处于断开状态时打开。

示例

```
anyconnect:disconnect
```

导入证书

使用此 URI 处理程序命令可将 PKCS12 编码的证书捆绑包导入到终端。AnyConnect 客户端使用终端上已安装的 PKCS12 编码的证书向 ASA 验证自身。仅支持 pkcs12 证书类型。

anyconnect:[//]**import**[/]**?type=pkcs12&uri=***http%3A%2F%2Fexample.com%2Fcertificatename.p12*

参数

- **type**- 仅支持 pkcs12 证书类型。
- **uri**- 在其中找到证书的 URL 编码的标识符。

示例

```
anyconnect:import?type=pkcs12&uri=http%3A%2F%2Fexample.com%2FCertName.p12
```

导入 VPN 客户端配置文件

使用此 URI 处理程序方法将客户端配置文件分发到 AnyConnect 客户端。

anyconnect:[//]**import**[/]**?type=profile&uri=***filename.xml*

示例

```
anyconnect:import?type=profile&uri=file%3A%2F%2Fsdcard%2Fprofile.xml
```

本地化 AnyConnect 用户界面和消息

使用此 URI 处理程序方法本地化 AnyConnect 客户端。

anyconnect:[//]**import**[/]**?type=localization&lang=***LanguageCode***&host=***ServerAddress*

参数

导入操作需要所有参数。

- **type**- 导入类型，本例中为本地化。
- **lang**- 长度为两个字符或四个字符的语言标记，表示 anyconnect.po 文件中提供的语言。例如，语言标记可能采用简化形式，fr 表示“法语”，fr-ca 表示“加拿大法语”。
- **host**- 输入 ASA 的域名或 IP 地址以匹配 AnyConnect 连接条目的 Server Address 字段。

示例

```
anyconnect:import?type=localization&lang=fr&host=asa.example.com
```

排除移动设备上的 AnyConnect 故障

开始之前

在移动设备上启用日志记录，并按照相应用户指南中的故障排除说明执行操作：

- Cisco AnyConnect Secure Mobility Client 用户指南 (Android)，版本 4.6
- Cisco AnyConnect Secure Mobility Client 用户指南 (Apple iOS)，版本 4.6.x
- Cisco AnyConnect Secure Mobility Client 用户指南，版本 4.1.x (Windows Phone)

如果遵循这些说明未能解决问题，请尝试以下操作：

步骤 1 确定在桌面客户端或其他移动操作系统上是否发生相同的问题。

步骤 2 确保在 ASA 中已安装适当的许可证。

步骤 3 如果证书身份验证失败，请检查以下项：

a) 确保选择了正确的证书。

b) 确保设备中的客户端证书将客户端身份验证作为扩展密钥使用。

c) 确保 AnyConnect 配置文件中的证书匹配规则不会过滤掉用户选择的证书。

即便用户选择了证书，如果该证书不匹配配置文件中的过滤规则，也不会使用它进行身份验证。

d) 如果身份验证机制使用与 ASA 关联的任何记账策略，请验证用户是否能够成功进行身份验证。

e) 如果您在期望使用仅证书身份验证时看到身份验证屏幕，请配置该连接以使用组 URL 并确保没有为隧道组配置辅助身份验证。

步骤 4 在 Apple iOS 设备上，请检查以下事项。

a) 如果在设备唤醒后 VPN 连接未恢复，请确保网络漫游已启用。

b) 如果使用按需连接，请验证已配置仅证书身份验证和组 URL。

下一步做什么

如果问题仍然存在，请在客户端上启用日志记录并在ASA中启用调试日志记录。有关详细信息，请参阅合适版本的 思科 ASA 5500-X 系列下一代防火墙配置指南。

第 12 章

思科 AnyConnect 客户体验反馈模块

注释 默认情况下，思科将收集您的私人和企业数据。

客户体验反馈 (CEF) 模块为我们提供有关客户使用和启用的功能和模块的信息。此信息将让我们了解用户体验，从而让思科继续改善 AnyConnect 的质量、可靠性、性能和用户体验。

有关信息收集和使用的详细信息，请参阅思科在线隐私声明要点页面，其中提供了 AnyConnect 安全移动客户端补充信息。 所有数据都以匿名方式收集，且不包含个人可识别数据。数据发送也将安全进行。

思科收集以下类型的数据：

- 使用情况数据 - 有关详细信息，请参阅隐私政策。此数据每月收集和发送一次。
- 网络威胁数据 - 发生威胁报告时即发送。
- 故障报告 - 每 24 小时检查一次 AnyConnect 生成的故障转储文件，收集并发送至客户体验反馈服务器。

客户体验反馈模块的主要组件如下：

- 反馈模块 - 用于收集信息并定期发送到服务器的 AnyConnect 软件组件。
- 思科反馈服务器 - 思科自有的云基础设施，用于收集客户体验反馈数据，并以原始格式存储在临时存储区中。

- 配置客户体验反馈， 第 283 页

配置客户体验反馈

AnyConnect 客户体验反馈模块随 AnyConnect 部署，默认启用。您可以通过创建客户体验反馈配置文件来修改发送的反馈，包括完全退出体验反馈。此方法是禁用反馈模块的首选方法，但您也可以在 AnyConnect 部署过程中删除它。

开始之前

客户体验反馈模块自动启用。

步骤 1 单独打开客户体验反馈配置文件编辑器或在 ASDM 中打开。导航到**配置 (Configuration)** > **远程访问 VPN (Remote Access VPN)** > **网络（客户端）访问 (Network [Client] Access)** > **AnyConnect 客户端配置文件 (AnyConnect Client Profile)**。

步骤 2 创建 AnyConnect 客户端配置文件，并且提供**反馈服务配置文件**的配置文件使用情况。

步骤 3 如果您不想提供反馈，请取消选中**启用客户体验反馈服务 (Enable customer Experience Feedback Service)**。

安装后可随时禁用反馈。

步骤 4 如果不想发送 AnyConnect 生成的故障报告，请取消选中**包含故障报告 (Include Crash Report)**。

默认包括故障报告。

步骤 5 输入您选择的客户密钥或 ID。

此 ID 可让思科识别您的组织的信息。

第 13 章

AnyConnect 故障排除

收集用于故障排除的信息

查看统计详细信息

管理员或最终用户可查看当前 AnyConnect 会话的统计信息。

步骤 1 在 Windows 上，导航到**高级窗口 > 统计信息 > VPN 文件夹**。在 Linux 上，单击用户 GUI 中的**详细信息 (Details)** 按钮。

步骤 2 根据客户端计算机上加载的软件包，从以下选项中进行选择。

- **Export Stats** - 将连接统计信息保存为一个文本文件，供以后分析和调试。
- **Reset** - 将连接信息重置为零。AnyConnect 将立即开始收集新数据。
- **Diagnostics** - 启动 AnyConnect 诊断和报告工具 (DART) 向导，该向导将捆绑指定日志文件和诊断信息，供客户端连接的分析和调试。

运行 DART 以收集用于故障排除的数据

DART 是 AnyConnect 诊断和报告工具，可用来收集数据以对 AnyConnect 安装和连接问题进行故障排除。DART 收集日志、状态和诊断信息，以供思科技术支持中心 (TAC) 分析。

DART 向导在运行 AnyConnect 的设备上运行。您可以从 AnyConnect 启动 DART 或不使用 AnyConnect 自行启动它。

注释 DART 需要 macOS、Ubuntu 18.04 和 Red Hat 7 的管理员权限才能收集日志。

此外，仅对于 ISE 终端安全评估，一旦发生 ISE 终端安全评估崩溃或终端变为不合规，您可以自动收集 DART（如果已配置）。要启用自动 DART，请将 DARTCount 设置为任意非零值。设置为 0 时，功能禁用。启用自动 DART 可防止因时间推移而导致数据丢失。在以下位置收集自动汇集的 DARTS：

- Windows — %LocalAppData%/Cisco/Cisco AnyConnect Secure Mobility Client
- macOS — ~/.cisco/iseposture/log

支持以下操作系统：

- Windows 的 ISE 安全评估代理
- macOS
- Linux

步骤 1 启动 DART：

- 对于 Windows 设备，请启动Cisco AnyConnect Secure Mobility Client。
- 对于 Linux 设备，请选择**应用程序 (Applications)** > **继承 (Internet)** > **思科 DART (Cisco DART)**

  或 /opt/cisco/anyconnect/dart/dartui。
- 对于 macOS 设备，请选择 **应用程序 (Applications)** > **思科 (Cisco)** > **思科 DART (Cisco DART)**。

步骤 2 单击**统计数据 (Statistics)** 选项卡，然后单击**诊断 (Diagnostics)**。

步骤 3 选择**默认 (Default)** 或**自定义 (Custom)** 捆绑创建。

- Default - 包括典型日志文件和诊断信息，例如 AnyConnect 日志文件、有关计算机的常规信息以及 DART 执行和不执行的功能的摘要。捆绑包的默认名称为 `DARTBundle.zip`，它会保存到本地桌面。
- Custom - 可指定要在捆绑中包含什么文件（或默认文件）和存储捆绑的位置。

  Linux 和 macOS 的成功路由和过滤更改不会记录在日志中，以便您可以更好地关注重要事件。否则，在系统日志事件速率限制下，重要事件可能减少和被忽视。此外，捕获过滤设置使您可以查看 macOS 的系统 pf 配置文件以及 AnyConnect 过滤配置文件。对于 Linux，即使对大多数这些配置的访问受限，iptables 和 ip6tables 输出也会显示在 DART 中，除非 DART 工具通过 sudo 运行。

注释　对于 macOS，只有**默认值 (Default)** 选项。您无法自定义捆绑包需要包括的文件。

注释　如果您选择**自定义 (Custom)**，则可以配置要在捆绑中包含哪些文件，并且为文件指定不同的存储位置。

步骤 4 如果DART似乎要花很长时间来收集默认文件列表，请单击**取消 (Cancel)**，重新运行DART，并选择**自定义 (Custom)**以选择较少的文件。

步骤 5 如果您选择**默认 (Default)**，DART 将开始创建捆绑包。如果您选择**自定义 (Custom)**，请继续按照向导提示指定日志、首选项文件、诊断信息和任何其他定制项。

在 DART 中显示 UDID

在 DART CLI 中，您可以显示客户端的唯一设备标识符 (UDID)。例如，对于 Windows，转到包含 dartcli.exe (C:\Program Files\Cisco\Cisco AnyConnect Secure Mobility Client) 的文件夹，然后输入 **dartcli.exe -u** 或 **dartclie.exe -udid**。

收集日志以收集关于安装或卸载问题的数据（适用于 Windows）

如果您遇到 AnyConnect 安装或卸载故障，需要收集日志，因为 DART 收集对此没有诊断能力。

在您解压 AnyConnect 文件的同一文件夹中运行 msiexec 命令：

- 对于安装故障，请输入

  ```
  C:/temp>msiexec /i anyconnect-win-version-pre-deploy-k9.msi /lvx c:/Temp/ac-install.log?
  ```

  其中 *c:/temp/ac-install.log?* 可以是您选择的文件名。

- 对于卸载故障，请输入

  ```
  c:/temp/msiexec /x anyconnect-win-version-pre-deploy-k9.msi /lvx c:/Temp/ac-install.log?
  ```

  其中 *c:/temp/ac-uninstall.log?* 可以是您选择的文件名。

注释　对于卸载故障，应该使用特定于当前已安装版本的 MSI。

您可以改变上述相同命令，以采集关于无法在 Windows 上正确安装或卸载的任何模块的信息。

获取计算机系统信息

对于 Windows，键入 **msinfo32 /nfo c:\msinfo.nfo**。

获取 Systeminfo 文件转储

对于 Windows，在 sysinfo 命令提示符中键入 **c:\sysinfo.txt**。

检查注册表文件

SetupAPI 日志文件中如下所示的条目表示找不到文件：

```
E122 Device install failed. Error 2: The system cannot find the file specified.
E154 Class installer failed. Error 2: The system cannot fine the file specified.
```

确保 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce 注册表项存在。若没有此注册表项，将禁止所有 inf 安装包。

AnyConnect 日志文件的位置

日志保留在以下文件中：

- Windows- `\Windows\Inf\setupapi.app.log or \Windows\Inf\setupapi.dev.log`

  注释 在 Windows 中，您必须使隐藏的文件可见。

  如果是初次网络部署安装，则日志文件位于每位用户的临时目录下：

  `%TEMP%\anyconnect-win-4.X.xxxxx-k9-install-yyyyyyyyyyyyyy.log`。

  如果升级来自于最佳网关推送，则日志文件位于以下位置：

  `%WINDIR%\TEMP\anyconnect-win-3.X.xxxxx-k9-install-yyyyyyyyyyyyyy.log`。

  获取适用于您要安装的客户端版本的最新文件。*xxx* 因版本而异，*yyyyyyyyyyyyy* 指定安装的日期和时间。

- MacOS （10.12 及更高版本）- 日志记录数据库；使用控制台应用或 log 命令查询 VPN、DART 或 Umbrella 的日志
- MacOS （基于旧版文件的日志）- `/var/log/system.log`（用于所有其他模块）
- Linux Ubuntu-`/var/log/syslog`
- Linux Red Hat-`/var/log/messages`

运行 DART 以清除故障排除数据

在 Windows 中，您可以使用 DART 向导清除生成的日志。

步骤 1 使用管理员权限启动 DART。

步骤 2 单击**清除所有日志 (Clear All Logs)** 以开始清除日志。

AnyConnect 连接或断开连接问题

AnyConnect 无法建立初始连接或未断开连接

问题：AnyConnect 不会建立初始连接，或者当您单击“Cisco AnyConnect 安全移动客户端”(Cisco AnyConnect Secure Mobility Client) 窗口上的“断开连接”(Disconnect) 时出现意外结果。

解决方案：进行以下检查

- 如果使用 Citrix 高级网关客户端版本 2.2.1，请删除 Citrix 高级网关客户端，直到 Citrix 解决 CtxLsp.dll 问题。
- 如果您使用具有 AT&T Sierra 无线 875 网卡的 AT&T 通信管理器 6.2 版或 6.7 版，请执行以下步骤解决此问题：
  1. 禁用 Aircard 加速。
  2. 启动 **AT&T Communication Manager > 工具 (Tools) > 设置 (Settings) > 加速 (Acceleration) > 启动 (Startup)**。
  3. 键入 **manual**。
  4. 单击**停止 (Stop)**。
- 从 ASA 获取配置文件，查找连接失败的标志：
  - 从 ASA 控制台键入 **write net x.x.x.x:ASA-Config.txt**，其中 *x.x.x.x* 是 TFTP 服务器在网络中的 IP 地址。
  - 从 ASA 的控制台，键入 **show running-config**。剪切并粘贴配置文件到文本编辑器并保存。
- 查看 ASA 事件日志：
  1. 在 ASA 控制台上，添加以下命令行以查看 ssl、webvpn、anyconnect 和 auth 事件：

     ```
     config terminal
     logging enable
     logging timestamp
     logging class auth console debugging
     logging class webvpn console debugging
     logging class ssl console debugging
     logging class anyconnect console debugging
     ```

  2. 尝试连接 AnyConnect 客户端，发生连接错误时，则将日志信息从控制台上剪切并粘贴至文本编辑器并保存。
  3. 键入 **no logging enable** 禁用日志记录。
- 使用 Windows 事件查看器从客户端计算机获取思科 AnyConnect VPN 客户端日志。
  1. 选择**开始 (Start) > 运行 (Run)** 并键入 **eventvwr.msc /s**。
  2. 在（Windows 7 的）应用和服务日志中找到思科 AnyConnect VPN 客户端，并选择**将日志文件另存为...**。。

3. 指定文件名，例如 AnyConnectClientLog.evt。您必须使用 .evt 文件格式。

- 修改 Windows 诊断调试实用程序。

1. 如 WinDbg 文档所示，附加 vpnagent.exe 进程。
2. 确定 IPv6/IPv4 IP 地址分配是否存在冲突。在事件日志中查找是否有已识别的冲突。
3. 如果发现冲突，则向要使用的客户端计算机注册表添加额外的路由调试。这些冲突在 AnyConnect 事件日志中可能会如下所示：

```
Function: CRouteMgr:modifyRoutingTable Return code: 0xFE06000E File: .\VpnMgr.cpp
Line:1122
Description: ROUTEMGR_ERROR_ROUTE_TABLE_VERIFICATION_FAILED.
Termination reason code 27: Unable to successfully verify all routing table
modifications are correct.

Function: CChangeRouteTable::VerifyRouteTable Return code: 0xFE070007
File: .\RouteMgr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
gr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
```

4. 通过添加特定的注册表项 (Windows) 或文件（Linux 和 macOS）为连接启用一次性的路由调试。

   - 在 32 位 Windows 中，DWORD 注册表值必须是 `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client\DebugRoutesEnabled`
   - 在 64 位 Windows 中，DWORD 注册表值必须是 `HKEY_LOCAL_MACHINE\Software\WOW6432node\Cisco\Cisco AnyConnect Secure Mobility Client\DebugRoutesEnabled`
   - 在 Linux 或 macOS 中，使用 sudo touch 命令在以下路径中创建文件：`/opt/cisco/anyconnect/debugroutes`

注释 密钥或文件将在启动隧道连接时删除。文件的密钥或内容的值不是重要的密钥时或文件足以启用调试。

启动 VPN 连接。找到此密钥或文件时，系统临时目录（在 Windows 中通常是 C:\Windows\Temp，在 macOS 或 Linux 中通常是 /opt/cisco/anyconnect）中将创建两个路由调试文本文件。如果已经存在这两个文件（debug_routechangesv4.txt4 和 debug_routechangesv6.txt），它们将会被覆盖。

AnyConnect 无法传输流量

问题：AnyConnect 客户端在连接后无法将数据发送到专用网络。

解决方案：进行以下检查

- 如果您使用具有 AT&T Sierra 无线 875 网卡的 AT&T 通信管理器 6.2 版或 6.7 版，请执行以下步骤解决此问题：
  1. 禁用 Aircard 加速。
  2. 启动 AT&T Communication Manager > 工具 (Tools) > 设置 (Settings) > 加速 (Acceleration) > 启动 (Startup)。
  3. 键入 **manual**。
  4. 单击**停止 (Stop)**。
- 获取 show vpn-sessiondb detail anyconnect filter name <username> 命令的输出。如果输出指定 Filter Name: XXXXX，则还要获取 show access-list XXXXX 命令的输出。验证 ACL 未阻止需要的流量。
- 从 AnyConnect VPN Client > Statistics > Details > Export 获取 DART 文件或输出 (AnyConnect-ExportedStats.txt)。观察统计、界面和路由表。
- 检查 ASA 配置文件中的 NAT 语句。如果已启用 NAT，则您必须排除从网络地址转换返回到客户端的数据。例如，要使 NAT 从 AnyConnect 池中排除 IP 地址，需要使用以下代码：

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

- 验证是否为设置启用了隧道化默认网关。传统默认网关是最不适合非解密流量的网关。

```
route outside 0.0.209.165.200.225
route inside 0 0 10.0.4.2 tunneled
```

  如果 VPN 客户端需要访问 VPN 网关路由表中未列出的资源，数据包将由标准默认网关传送。VPN 网关不需要完整的内部路由表。如果您使用隧道化关键字，则路由将处理来自 IPsec/SSL VPN 连接的解密流量。标准流量通常不会路由到 209.165.200.225，而来自 VPN 的流量将路由到 10.0.4.2 且已进行解密。
- 在使用 AnyConnect 建立隧道前后，收集 ipconfig /all 的文本转储和路由打印输出。
- 在客户端上执行网络数据包捕获，或在 ASA 上启用捕获。

注释 如果某些应用（例如 Microsoft Outlook）无法使用隧道，则在具有 ping 扩展集的网络中 ping 已知设备，可查看接受的大小（例如，ping -| 500，ping -| 1000，ping -| 1500，以及 ping -| 2000）。从 ping 结果中可对网络中的分段问题略知一二。然后，您可以为存在分段问题的用户配置一个特殊组，并将该组的 anyconnect mtu 设置为 1200。您也可从旧 IPsec 客户端复制 Set MTU.exe 实用程序，并强制将物理适配器 MTU 设置为 1300。重启后，查看是否有区别。

基于 VM 的子系统的连接问题

如果主机（Windows 10 或 macOS Big Sur）上的 AnyConnect VPN 处于活动状态，而适用于 Linux (WSL2) 或VMware Fusion VM 的 Windows 子系统遇到了连接问题，请按照以下步骤配置仅限于虚拟适配器的本地 LAN 拆分排除隧道子网。

步骤 1 在 ASDM 中，导航到**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络[客户端]访问 (Network [Client] Access) > 高级 (Advanced) > AnyConnect 定制属性 (AnyConnect Custom Attributes)** 以配置新的自定义属性类型。

步骤 2 选择 **Add**（添加）并在“创建自定义属性”(Create Custom Attribute) 窗格中设置以下项：

a) 输入 **BypassVirtualSubnetsOnlyV4** (IPv4) 或 **BypassVirtualSubnetsOnlyV6** (IPv6) 作为新的类型。

b) 或者，输入说明。

c) 在 **AnyConnect 自定义属性名称 (AnyConnect Custom Attributes Names)** 中将名称和值设置为 *true*。

如果已在组策略中为特定 IP 协议配置了本地 LAN 通配符拆分排除，则客户端会将其限制为仅虚拟子网，但前提是同一 IP 协议启用了自定义属性。如果本地 LAN 通配符拆分排除未在组策略中配置，则由客户端为启用了自定义属性的 IP 协议添加，从而会导致相应地实施受限的本地 LAN 拆分排除。在未配置其他拆分-排除网络的情况下，所有物理适配器流量都将通过隧道传输，即类似于全隧道配置。

步骤 3 通过以下方式将先前创建的自定义属性类型和名称附加到组策略中：**配置 (Configuration) > 远程访问 VPN (Remote Access VPN) > 网络（[客户端）访问 Network [Client] Access > 组策略 (Group Policies) > 编辑 (Edit) > 高级 (Advanced) > AnyConnect 客户端 (AnyConnect Client) > 自定义属性 (Custom Attributes)**。

下一步做什么

要验证属性值是否设置正确，请检查 AnyConnect VPN 日志中是否存在以“已收到 VPN 会话配置”(Received VPN Session Configuration) 开头的消息。它应指明本地 LAN 通配符仅限于虚拟子网。

VPN 服务故障

VPN 服务连接失败

问题：您收到“Unable to Proceed, Cannot Connect to the VPN Service”消息。AnyConnect 的 VPN 服务未运行。

解决方案：确定是否有另一个应用与该服务冲突。请参阅确定服务的冲突项。

确定服务的冲突项

以下过程确定冲突是在启动时针对服务器的初始化还是针对其他运行的服务，例如，因为服务启动失败。

步骤 1 查看 Windows 管理工具下的服务，以确保思科 AnyConnect VPN 代理未运行。如果它正在运行并且仍然显示错误消息，则可能需要禁用甚至卸载工作站上的另一个 VPN 应用。在执行该操作后，重新启动，然后重复此步骤。

步骤 2 尝试启动思科 AnyConnect VPN 代理。

步骤 3 在事件查看器中检查 AnyConnect 日志以查找是否存在指出服务无法启动的消息。请注意步骤 2 的手动重新启动的时间戳以及工作站启动时的时间戳。

步骤 4 在事件查看器中检查系统和应用日志以查找任何冲突消息的相同通用时间戳。

步骤 5 如果日志指示启动服务失败，请查找在大致相同时间戳的其他信息性消息，这些消息指示以下情况之一：

- 文件缺失 - 从独立 MSI 安装重新安装 AnyConnect 客户端以排除缺失的文件。
- 另一相关服务中的延迟 - 禁止启动活动以缩短工作站的启动时间。
- 与另一应用或服务的冲突 - 确定是否另一项服务在侦听 vpnagent 使用的同一端口，或者是否某些 HIDS 软件阻止我们的软件侦听某个端口。

步骤 6 如果日志没有直接指向某个原因，请使用试错法来识别冲突。识别了最可能的候选项后，请从服务面板禁用这些服务（例如 VPN 产品、HIDS 软件、Spybot 清除程序、嗅探器、防病毒软件等）。

步骤 7 重新启动。如果 VPN 代理服务仍无法启动，请开始关闭操作系统的默认安装未安装的服务。

VPN 客户端驱动程序遇到错误（Microsoft Windows 更新后）

问题：如果您最近更新了 Microsoft certclass.inf 文件，在尝试建立 VPN 连接时会出现以下消息：

```
The VPN client driver has encountered an error.
```

如果检查 C:\WINDOWS\setupapi.log，会看到以下错误：

```
#W239 The driver signing class list “C:\WINDOWS\INF\certclass.inf” was missing or invalid.
 Error 0xfffffbf8: Unknown Error. Assuming all device classes are subject to driver signing
 policy.
```

解决方案：在命令提示符下输入 **C:\>systeminfo** 或查看 C:\WINDOWS\WindowsUpdate.log，可查看最近安装了哪些更新。按照说明修复 VPN 驱动程序。

修复 VPN 客户端驱动程序错误

尽管执行的上述步骤可能表明目录未损坏，但密钥文件仍可能已被未签名的文件覆盖。如果此故障仍然存在，请通过向 Microsoft 提交案例来确定驱动程序签名数据库为什么损坏。

步骤 1 以管理员身份打开命令提示符。

步骤 2 输入 **net stop CryptSvc**。

步骤 3 分析数据库，通过输入 **esentutl /g %systemroot%\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb** 验证其有效性或将目录 %/WINDIR%\system32\catroot2 重命名为 catroot2_old。

步骤 4 出现提示时，选择**确定 (OK)** 尝试修复。退出命令提示符并重新启动。

驱动程序故障

修复 VPNVA.sys 中的驱动程序故障

问题：VPNVA.sys 驱动程序故障。

解决方案：找到被绑定到 Cisco AnyConnect 虚拟适配器的中间驱动程序，并取消选择它们。

修复 vpnagent.exe 中的驱动程序故障

步骤 1 创建名为 c:\vpnagent 的目录。

步骤 2 查看任务管理器中的“流程”(Process) 选项卡，确定 vpnagent.exe 中的进程 PID。

步骤 3 打开命令提示符并更改安装了调试工具的目录。默认情况下，Windows 的调试工具位于 `C:\Program Files\Debugging Tools`。

步骤 4 键入 **cscript vpnagent4.vbs -crash -p PID -o c:\vpnagent -nodumponfirst**，其中 *PID* 是 **vpnagent.exe** 的 PID。

步骤 5 使打开的窗口以最小化状态运行。监控时不可注销系统。

步骤 6 当发生故障时，将 c:\vpnagent 的内容压缩为 zip 文件。

步骤 7 使用 **!analyze -v** 进一步诊断 crashdmp 文件。

网络访问管理器的链路/驱动程序问题

如果网络访问管理器无法识别有线适配器，请尝试将网线拔出并重新插入。如果这无法解决问题，则链路可能有问题。网络访问管理器可能无法确定适配器的正确链路状态。请检查 NIC 驱动程序的连接属性。您可能在高级面板中看到“等待链路”(Wait for Link) 选项。设置为“开”(On) 时，有线 NIC 驱动程序初始化代码等待自动协商完成，再确定连接是否有效。

其他故障

AnyConnect 故障

问题：在系统重启后，您收到 the system has recovered from a serious error 消息。

解决方案：从 %temp% 目录（例如 C:\DOCUME~1\jsmith\LOCALS~1\Temp）中收集生成的 .log 和 .dmp 文件。复制文件或备份文件。请参阅如何备份 .log 或 .dmp 文件。

如何备份 .log 或 .dmp 文件

步骤 1 从“开始 > 运行”菜单运行名为 Dr. Watson (Drwtsn32.exe) 的 Microsoft 实用程序。

步骤 2 进行以下配置并单击**确定 (OK)**：

```
Number of Instructions     : 25
Number of Errors to Save : 25
Crash Dump Type   : Mini
Dump Symbol Table : Checked
Dump All Thread Contexts : Checked
Append to Existing Log File : Checked
Visual Notification : Checked
Create Crash Dump File : Checked
```

步骤 3 在客户端计算机上的“开始 > 运行”菜单中输入 **eventvwr.msc /s**，以从 Windows 事件查看器中获取思科 AnyConnect VPN 客户端日志。

步骤 4 在（Windows 7 的）应用和服务日志中找到**思科 AnyConnect VPN 客户端**，并选择**将日志文件另存为...**。。以 .evt 文件格式分配文件名，例如 AnyConnectClientLog.evt。

vpndownloader 中的 AnyConnect 故障（分层服务提供商 (LSP) 模块和 NOD32 AV）

问题：AnyConnect 在尝试建立连接时成功进行身份验证并建立了 SSL 会话，但随后在使用 LSP 或 NOD32 AV 时，AnyConnect 客户端在 vpndownloader 中发生故障。

解决方案：删除 2.7 版中的 Internet Monitor 组件，并升级到 ESET NOD32 AV 3.0 版。

蓝屏（AT&T 拨号器）

问题：如果您使用 AT&T 拨号器，则客户端操作系统有时会出现蓝屏，导致创建微型转储文件。

解决方案：升级到最新的 7.6.2 AT&T 全球网络客户端。

安全告警

Microsoft Internet Explorer 安全告警

问题：Microsoft Internet Explorer 中出现安全告警窗口，其中包含以下文字：

```
Information you exchange with this site cannot be viewed or changed by others. However,
there is a problem with the site's security certificate. The security certificate was issued
 by a company you have not chosen to trust. View the certificate to determine whether you
want to trust the certifying authority.
```

解决方案：连接到未识别为受信任网站的ASA时可能出现此告警。为防止出现此告警，请在客户端上安装一个受信任根证书。请参阅在客户端上安装受信任根证书。

“未知授权认证”(Certified by an Unknown Authority) 告警

问题：在浏览器中可能出现 Web Site Certified by an Unknown Authority 告警窗口。Security Alert 窗口的上半部分显示以下文本：

```
Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.
```

解决方案：在连接到不被识别为受信任站点的ASA时可能出现此安全告警。为防止出现此告警，请在客户端上安装一个受信任根证书。请参阅在客户端上安装受信任根证书。

在客户端上安装受信任根证书

开始之前

生成或获取将用作受信任根证书的证书。

注释 您可以通过将自签名证书安装为客户端上的受信任根证书，在短期内避免出现安全证书警告。但是我们不建议这样做，因为用户可能会无意中将浏览器配置为信任欺诈服务器上的证书，并且在连接到安全网关时可能不得不响应安全警告而给用户带来不便。

步骤 1 单击“安安全警报”(Security Alert) 窗口中的**查看证书 (View Certificate)**。

步骤 2 单击**安装证书 (Install Certificate)**。

步骤 3 单击**下一步 (Next)**。

步骤 4 选择**将所有证书放入下列存储 (Place all certificates in the following store)**。

步骤 5 单击**浏览 (Browse)**。

步骤 6 在下拉列表中，选择**受信任的根证书颁发机构 (Trusted Root Certification Authorities)**。

步骤 7 遵循证书导入向导提示继续操作。

掉线的连接

无线连接在引入有线连接时掉线（Juniper Odyssey 客户端）

问题：在 Odyssey 客户端上启用无线抑制后，如果引入有线连接，那么无线连接就会掉线。禁用无线抑制后，无线连接如预期的那样运行正常。

解决方案：配置 Odyssey 客户端。

配置 Odyssey 客户端

步骤 1 在 Network Connections 中，复制适配器的名称（与在其连接属性中显示的一样）。如果您编辑注册表，请先进行备份，然后再进行任何更改。一定要谨慎，因为如果修改错误，可能导致严重问题。

步骤 2 打开注册表并转到 HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.\odyssey\client\configuration\options\adapterType\virtual。

步骤 3 在 virtual 下创建新的字符串值。将适配器的名称从 Network 属性复制到注册表部分。额外的注册表设置一旦保存，就会在创建客户端 MSI 并下推到其他客户端时通过端口传递。

连接 ASA 失败 (Kaspersky AV Workstation 6.x)

问题：安装 Kaspersky 6.0.3 后（即使已禁用），到 ASA 的 AnyConnect 连接会在 CSTP state = CONNECTED 之后立即失败。系统会显示以下消息：

```
SVC message: t/s=3/16: Failed to fully establish a connection to the secure gateway (proxy
 authentication, handshake, bad cert, etc.).
```

解决方案：卸载 Kaspersky 并访问其论坛获得其他更新。

没有 UDP DTLS 连接 (McAfee Firewall 5)

问题：使用 McAfee Firewall 5 时，UDP DTLS 连接无法建立。

解决方案：在 McAfee Firewall 中央控制台中，选择**高级任务 (Advanced Tasks)** > **高级选项和日志记录 (Advanced options and Logging)**，然后取消选中 McAfee Firewall 中的**自动阻止传入的片段 (Block incoming fragments automatically)** 复选框。

连接主机设备失败（Microsoft 路由和远程访问服务器）

问题：如果使用 RRAS，则当 AnyConnect 尝试建立到主机设备的连接时，事件日志中会记录以下终止错误：

```
Termination reason code 29 [Routing and Remote Access service is running]
The Windows service “Routing and Remote Access” is incompatible with the Cisco AnyConnect
 VPN Client.
```

解决方案：禁用 RRAS 服务。

连接失败/缺少凭证（负载均衡器）

问题：由于缺少凭证而连接失败。

解决方案：第三方负载均衡器无法洞悉 ASA 设备上的负载。因为 ASA 中的负载均衡功能足够智能，能够在设备之间均衡地分配 VPN 负载，所以我们建议使用内部 ASA 负载均衡。

安装故障

若未找到根本原因，则不要编辑 Windows 注册表

如果您在安装、卸载或升级 AnyConnect 时收到故障消息，我们不建议直接修改 Windows 安装程序注册表项，否则可能会导致意外后果。确定正确的根本原因后，Microsoft 提供的工具可以对安装程序问题进行故障排除。

AnyConnect 无法下载 (Wave EMBASSY Trust Suite)

问题：AnyConnect 客户端无法下载，并出现以下错误消息：

```
“Cisco AnyConnect VPN Client Downloader has encountered a problem and needs to close.”
```

解决方案：将补丁更新上传到 1.2.1.38 版以解决所有 dll 问题。

不兼容问题

更新路由表失败（Bonjour 打印服务）

问题：如果您使用的是 Bonjour 打印服务，AnyConnect 事件日志会指出识别 IP 转发表失败。

解决方案：通过在命令提示符下键入 **net stop “bonjour service”** 禁用 BonJour 打印服务。Apple 公司已经推出了新版 mDNSResponder (1.0.5.11)。要解决此问题，请将新版 Bonjour 捆绑至 iTunes，且作为单独程序从 Apple 网站下载。

TUN 的版本不兼容（OpenVPN 客户端）

问题：错误表示此系统上已安装 TUN 版本，但该版本与 AnyConnect 客户端不兼容。

解决方案：卸载 Viscosity OpenVPN 客户端。

Winsock 目录冲突（LSP 症状 2 冲突）

问题：如果客户端上有 LSP 模块，可能会发生 Winsock 目录冲突。

解决方案：卸载 LSP 模块。

数据吞吐慢（LSP 症状 3 冲突）

问题：在 Windows 7 系统中使用 NOD32 Antivirus V4.0.468 x64 时可能出现数据吞吐慢。

解决方案：禁用 SSL 协议扫描。请参阅禁用 SSL 协议扫描。

禁用 SSL 协议扫描

步骤 1 转至“高级设置”(Advanced Setup) 中的 **协议过滤 (Protocol Filtering)** > **SSL** 并启用 SSL 协议扫描。

步骤 2 转到 **Web 访问保护 (Web access protection)** > **HTTP**、**HTTPS**，并选中 **不使用 HTTPS 协议检查 (Do not use HTTPS protocol checking)**。

步骤 3 返回到**协议过滤 (Protocol Filtering)** > **SSL** 并禁用 **SSL 协议扫描 (SSL protocol scanning)**。

DPD 失败（EVDO 无线网卡和 Venturi 驱动程序）

问题：如果客户端断开连接时您使用的是 EVDO 无线网卡和 Venturi 驱动程序，则事件日志会报告如下内容：

```
%ASA-5-722037: Group <Group-Name> User <User-Name> IP <IP-Address> SVC closing connection:
 DPD failure.
```

解决方案

- 检查应用、系统和 AnyConnect 事件日志中的相关断开连接事件，同时确定是否应用了 NIC 卡重置。
- 确保 Venturi 驱动程序为最新版本。在 6.7 版本的 AT&T 通信管理器中禁用 **Use Rules Engine**。

DTLS 流量失败（DSL 路由器）

问题：如果您与 DSL 路由器连接，则即使成功协商，DTLS 流量也可能会失败。

解决方案：连接到采用出厂设置的 Linksys 路由器。此设置支持稳定的 DTLS 会话且 ping 过程中无中断。添加规则以允许 DTLS 返回流量。

NETINTERFACE_ERROR（CheckPoint 和其他第三方软件，如 Kaspersky）

问题：尝试在用于建立 SSL 连接的计算机网络上检索操作系统信息时，AnyConnect 日志可能指示未能完全建立到安全网关的连接。

解决方案

- 如果是卸载完整性代理，然后安装 AnyConnect，请启用 TCP/IP。
- 确保如果在完整性代理安装上禁用 SmartDefense，则选中 TCP/IP。
- 如果在检索网络接口信息时第三方软件拦截或以其他方式阻止操作系统 API 调用，请检查是否有可疑的 AV、FW、AS 等。
- 确认设备管理器中只出现一个 AnyConnect 适配器实例。如果只有一个实例，则使用 AnyConnect 进行身份验证，并在 5 秒后手动从设备管理器启用适配器。
- 如果在 AnyConnect 适配器中启用了任何可疑的驱动程序，在“Cisco AnyConnect VPN 客户端连接”(Cisco AnyConnect VPN Client Connection) 窗口中取消选中它们予以禁用。

性能问题（虚拟机网络服务驱动程序）

问题：在某些虚拟机网络服务设备上使用 AnyConnect 时，会导致性能问题。

解决方案：取消选中 AnyConnect 虚拟适配器中所有即时消息设备的绑定。应用 dsagent.exe 驻留在 C:\Windows\System\dgagent 中。虽然其未出现在进程列表中，您可以用 TCPview (sysinternals) 打开套接字进行查看。当您终止此进程时，AnyConnect 将恢复正常运行。

已知的第三方应用冲突

我们已经知道，以下第三方应用获取Cisco AnyConnect Secure Mobility Client存在困难：

- Adobe 和苹果公司 - Bonjour 打印服务
  - Adobe Creative Suite 3
  - BonJour 打印服务
  - iTunes
- AT&T 通信管理器版本 6.2 和 6.7
  - AT&T Sierra 无线 875 卡
- AT&T 全球拨号器

- Citrix 高级网关客户端版本 2.2.1
- 防火墙冲突
  - 第三方防火墙可能会干扰 ASA 组策略中配置的防火墙功能。
- Juniper Odyssey 客户端
- Kaspersky AV 工作站 6.x
- McAfee 防火墙 5
- Microsoft Internet Explorer 8
- Microsoft 路由和远程接入服务器
- OpenVPN 客户端
- 负载均衡
- Wave EMBASSY Trust Suite
- 分层服务提供商 (LSP) 模块和 NOD32 AV
- EVDO 无线网卡和 Venturi 驱动程序
- DSL 路由器
- CheckPoint 和其他第三方软件（如卡巴斯基）
- 虚拟机网络服务驱动程序

第 14 章

附录：与 macOS 11 (Big Sur) 相关的 AnyConnect 更改

您必须为 macOS 11 运行 AnyConnect 4.9.04xxx（或更高版本）。它利用 macOS 中可用的系统扩展框架，而之前使用的是现在已弃用的内核扩展框架。由于这一变化，管理员必须批准 AnyConnect 系统扩展，并要能够确认这些更新的正确操作。此外，如果遇到严重的系统扩展（或相关的操作系统框架）问题，作为最后的变通方法，您可以按照故障转移至 AnyConnect 内核扩展的步骤进行操作，但这仅出于此目的而安装且不会再默认使用

关于 AnyConnect 系统扩展

AnyConnect 在 macOS 11 上使用网络系统扩展，捆绑在名为 Cisco AnyConnect Socket Filter 的应用程序中。该应用程序会控制扩展的激活和停用，并安装在 /Applications/Cisco 下。

AnyConnect 扩展包含以下三个组件，可在 macOS 系统首选项 - 网络用户界面窗口中显示：

- DNS 代理
- 应用程序/透明代理
- 内容过滤器

AnyConnect 要求其系统扩展及其所有组件就能处于活动状态方可正常运行，这意味着上述组件全部安装到位，并在 macOS 网络用户界面的左窗格中显示为绿色（正在运行）。

批准 AnyConnect 系统扩展

macOS 11 要求最终用户进行扩展审批或无需最终用户审批的 MDM 审批，然后才能运行系统扩展。AnyConnect 系统扩展需要两个审批：

- 批准系统扩展加载/激活 ，第 304 页
- 使用 MDM 批准系统扩展 ，第 305 页

批准系统扩展加载/激活

按照操作系统提示或更明确的 AnyConnect 通知应用程序的说明，批准 AnyConnect 系统扩展及其内容过滤器组件。

SUMMARY STEPS

1. 当您收到“系统扩展已阻止”(System Extension Blocked) 应用程序消息时，单击 AnyConnect 通知应用程序中的**打开首选项 (Open Preferences)** 按钮或**打开安全首选项 (Open Security Preferences)** 按钮。您还可以导航到“系统首选项”(System Preferences) 应用程序并转到“安全和隐私”(Security&Privacy) 窗口。
2. 单击左下角的锁，然后提供请求的凭证以解锁并允许更改。
3. 单击安全和隐私窗口中的**允许 (Allow)**，接受思科 AnyConnect 套接字过滤器。

DETAILED STEPS

步骤 1 当您收到“系统扩展已阻止”(System Extension Blocked) 应用程序消息时，单击 AnyConnect 通知应用程序中的**打开首选项 (Open Preferences)** 按钮或**打开安全首选项 (Open Security Preferences)** 按钮。您还可以导航到“系统首选项”(System Preferences) 应用程序并转到“安全和隐私”(Security&Privacy) 窗口。

步骤 2 单击左下角的锁，然后提供请求的凭证以解锁并允许更改。

步骤 3 单击安全和隐私窗口中的**允许 (Allow)**，接受思科 AnyConnect 套接字过滤器。

当多个系统扩展需要审批时，按钮标记为“详细信息...”(Details...)。。在这种情况下，单击**详细信息...(Details...)**，选中**思科 AnyConnect 套接字过滤器 (Cisco AnyConnect Socket Filter)** 复选框，单击**确定 (OK)**，然后批准需要“允许”(Allow) 的任何后续提示。

下一步做什么

当扩展程序的内容过滤器组件获得批准时，您将收到通知。

使用 MDM 批准系统扩展

使用管理配置文件具有以下设置的 SystemExtensions 负载来批准 AnyConnect 系统扩展而无需最终用户交互：

特性	值
团队标识符	DE8Y96K9QP
捆绑包标识符	com.cisco.anyconnect.macos.acsockext
系统扩展类型	NetworkExtension

使用以下 WebContentFilter 负载设置来批准扩展的内容过滤器组件：

特性	值
AutoFilterEnabled	false
FilterBrowsers	false
FilterSockets	true
FilterPackets	false
FilterGrade	防火墙
FilterDataProviderBundleIdentifier	com.cisco.anyconnect.macos.acsockext
FilterDataProviderDesignatedRequirement	anchor apple generic and identifier "com.cisco.anyconnect.macos.acsockext" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = DE8Y96K9QP)
PluginBundleID	com.cisco.anyconnect.macos.acsockext
VendorConfig	
UserDefinedName	思科 AnyConnect 内容过滤器

确认激活 AnyConnect 系统扩展

要确认 AnyConnect 系统扩展是否已获批准并激活，请运行 **systemextensionsctl list** 命令：

```
% systemextensionsctl list
1 extension(s)
--- com.apple.system_extension.network_extension
enabled active teamID bundleID (version) name [state]
* * DE8Y96K9QP com.cisco.anyconnect.macos.acsockext
```

```
(4.9.03038/4.9.03038) Cisco AnyConnect Socket Filter Extension
[activated enabled]
```

您还可以检查系统首选项网络 UI 以确认所有三个 AnyConnect 扩展组件是否均已激活。

停用 AnyConnect 扩展

在 AnyConnect 卸载期间，系统会提示用户输入管理员凭证，以便批准停用系统扩展。

故障转移到内核扩展

AnyConnect 仍在 macOS11 上安装其内核扩展；但如果出现严重的系统扩展（或相关操作系统框架）问题或在思科技术支持中心 (TAC) 的指示下，您应仅将其用作回退。在 macOS 11 上加载之前，内核扩展需要通过 MDM 审批。最终用户审批不再可供选择。

开始之前

仅将这些步骤用作最后的解决方法。

SUMMARY STEPS

1. 使用管理配置文件的 *SystemPolicyKernelExtensions* 负载通过以下设置来批准 AnyConnect 内核扩展：
2. 运行以下会导致 AnyConnect 停用系统扩展并开始使用内核扩展的命令。系统将提示您输入管理员凭证。**% sudo launchctl unload /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist && /Applications/Cisco/Cisco\ AnyConnect\ Socket\ Filter.app/Contents/MacOS/Cisco\ AnyConnect\ Socket\ Filter -deactivateExt && echo kext=1 | sudo tee /opt/cisco/anyconnect/acsock.cfg && sudo launchctl load /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plis**
3. 运行以下命令以验证是否已加载内核扩展：**% kextstat | grep com.cisco.kext.acsock**

DETAILED STEPS

步骤 1 使用管理配置文件的 *SystemPolicyKernelExtensions* 负载通过以下设置来批准 AnyConnect 内核扩展：

特性	值
团队标识符	DE8Y96K9QP
捆绑包标识符	com.cisco.kext.acsock

MDM 配置文件将进行安装。

步骤 2 运行以下会导致 AnyConnect 停用系统扩展并开始使用内核扩展的命令。系统将提示您输入管理员凭证。**% sudo launchctl unload /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist && /Applications/Cisco/Cisco\ AnyConnect\ Socket\ Filter.app/Contents/MacOS/Cisco\ AnyConnect\ Socket\ Filter -deactivateExt && echo kext=1**

| sudo tee /opt/cisco/anyconnect/acsock.cfg && sudo launchctl load /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plis

步骤 3 运行以下命令以验证是否已加载内核扩展：**% kextstat | grep com.cisco.kext.acsock**

如果 AnyConnect 无法加载其内核扩展，请执行重新引导。

恢复到系统扩展

如果思科 TAC 确认修复了系统扩展问题（并消除了故障转移到内核扩展的需求），则可运行以下命令，指示 AnyConnect 切换回系统扩展：

```
% sudo launchctl unload /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist && sudo
 kextunload -b com.cisco.kext.acsock && sudo rm /opt/cisco/anyconnect/acsock.cfg && sudo
launchctl load /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist
```

通过修复程序安装 AnyConnect 或 macOS 版本。

AnyConnect 系统和内核扩展批准的示例 MDM 配置文件

使用以下 MDM 配置文件来加载 AnyConnect 系统和内核扩展，包括系统扩展的内容过滤器组件。

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">

      <dict>

      <key>PayloadContent</key>

      <array>

            <dict>

                  <key>AllowUserOverrides</key>

                  <true/>

                  <key>AllowedKernelExtensions</key>

                  <dict>

                        <key>DE8Y96K9QP</key>

                        <array>

                        <string>com.cisco.kext.acsock</string>

                        </array>

                  </dict>

                  <key>PayloadDescription</key>
```

```
        <string></string>
        <key>PayloadDisplayName</key>
        <string>AnyConnect Kernel Extension</string>
        <key>PayloadEnabled</key>
        <true/>
        <key>PayloadIdentifier</key>
        <string>37C29CF2-A783-411D-B2C7-100EDDFBE223</string>
        <key>PayloadOrganization</key>
        <string>Cisco Systems, Inc.</string>
        <key>PayloadType</key>
        <string>com.apple.syspolicy.kernel-extension-policy</string>
        <key>PayloadUUID</key>
        <string>37C29CF2-A783-411D-B2C7-100EDDFBE223</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
    </dict>
    <dict>
        <key>AllowUserOverrides</key>
        <true/>
        <key>AllowedSystemExtensions</key>
        <dict>
            <key>DE8Y96K9QP</key>
            <array>
            <string>com.cisco.anyconnect.macos.acsockext</string>
            </array>
        </dict>
        <key>PayloadDescription</key>
        <string></string>
        <key>PayloadDisplayName</key>
        <string>AnyConnect System Extension</string>
        <key>PayloadEnabled</key>
        <true/>
```

```
            <key>PayloadIdentifier</key>
            <string>A8364220-5D8D-40A9-Af66-1Fbfef94E116</string>
            <key>PayloadOrganization</key>
            <string>Cisco Systems, Inc.</string>
            <key>PayloadType</key>
            <string>com.apple.system-extension-policy</string>
            <key>PayloadUUID</key>
            <string>A8364220-5D8D-40A9-Af66-1Fbfef94E116</string>
            <key>PayloadVersion</key>
            <integer>1</integer>
        </dict>
        <dict>
            <key>Enabled</key>
            <true/>
            <key>AutoFilterEnabled</key>
            <false/>
            <key>FilterBrowsers</key>
            <false/>
            <key>FilterSockets</key>
            <true/>
            <key>FilterPackets</key>
            <false/>
            <key>FilterType</key>
            <string>Plugin</string>
            <key>FilterGrade</key>
            <string>firewall</string>
            <key>PayloadDescription</key>
            <string></string>
            <key>PayloadDisplayName</key>
            <string>Cisco AnyConnect Content Filter</string>
            <key>PayloadIdentifier</key>
<string>com.apple.webcontent-filter.339Ec532-9Ada-480A-Bf3D-A535F0F0B665</string>
```

```
                    <key>PayloadType</key>
                    <string>com.apple.webcontent-filter</string>
                    <key>PayloadUUID</key>
                    <string>339Ec532-9Ada-480A-Bf3D-A535F0F0B665</string>
                    <key>PayloadVersion</key>
                    <integer>1</integer>
                    <key>FilterDataProviderBundleIdentifier</key>
                    <string>com.cisco.anyconnect.macos.acsockext</string>
                    <key>FilterDataProviderDesignatedRequirement</key>
                    <string>anchor apple generic and identifier
"com.cisco.anyconnect.macos.acsockext" and (certificate leaf[field.1.2.840.113635.100.6.1.9]
 /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
 leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
DE8Y96K9QP)</string>
                    <key>PluginBundleID</key>
                    <string>com.cisco.anyconnect.macos.acsock</string>
                    <key>UserDefinedName</key>
                    <string>Cisco AnyConnect Content Filter</string>
                </dict>
        </array>
        <key>PayloadDescription</key>
        <string></string>
        <key>PayloadDisplayName</key>
        <string>Approved AnyConnect System and Kernel Extensions</string>
        <key>PayloadEnabled</key>
        <true/>
        <key>PayloadIdentifier</key>
        <string>A401Bdc2-4Ab1-4406-A143-11F077Baf52B</string>
        <key>PayloadOrganization</key>
        <string>Cisco Systems, Inc.</string>
        <key>PayloadRemovalDisallowed</key>
        <true/>
        <key>PayloadScope</key>
        <string>System</string>
```

```
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadUUID</key>
        <string>A401Bdc2-4Ab1-4406-A143-11F077Baf52B</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
</dict>
</plist>
```